mobey forum
mobile financial services

Mobey Forum's Biometrics Survey Results

July 2015

Produced by Mobey Forum’s Biometrics Workgroup

Workgroup chairs:

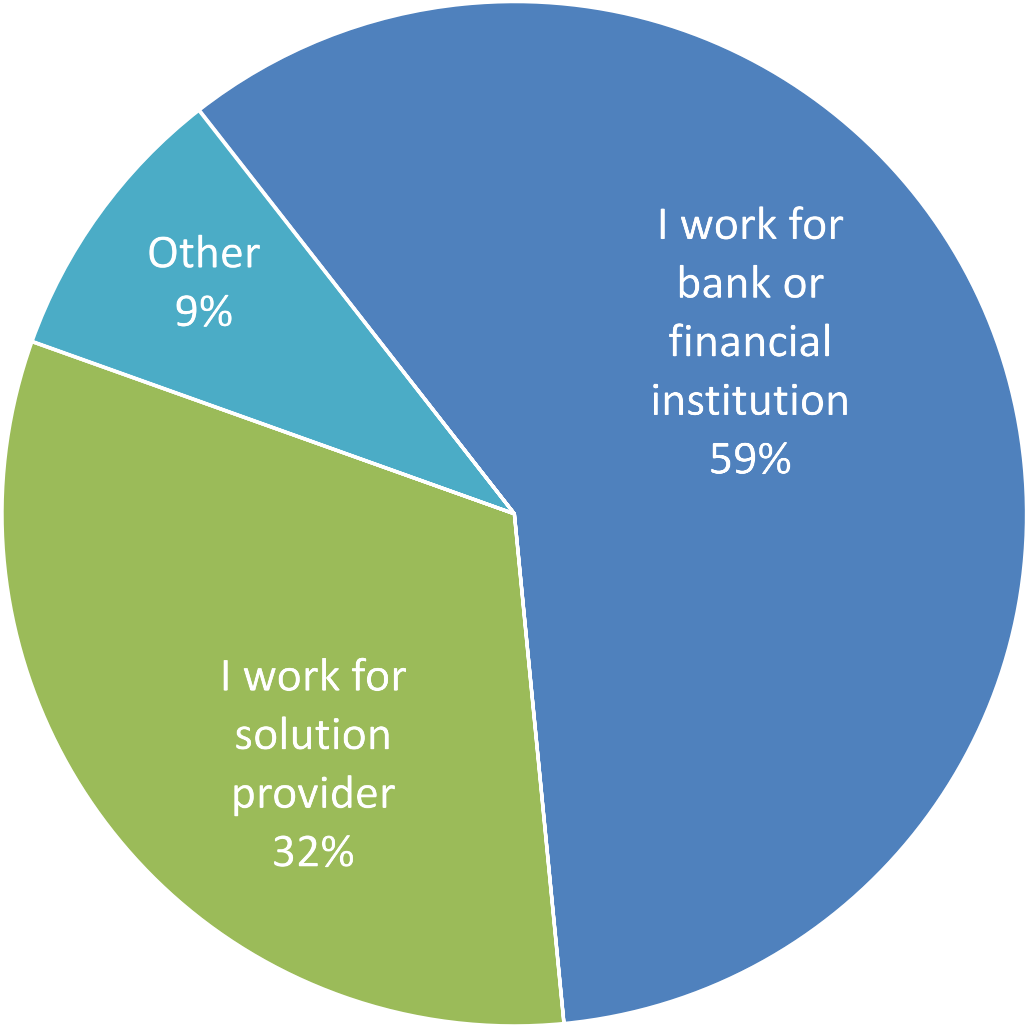
Mario Maawad, **CaixaBank** and Philippe Le Pape, **Morpho**

Jannicke	Birkevold	**DNB**
Evgeniy	Bondarenko	**Intervale**
Alec	Brusilovsky	**Trusted Computer Group**
Bhaskar	Chaudhary	**Mahindra Comviva**
Carlin	Covey	**Trusted Computer Group**
Eduardo	Galvao	**SIBS**
Yuri	Grin	**Intervale**
Andreas	Havsberg	**Nordea**
Hans	Illstad	**EVRY**
Nitin	Jain	**Mahindra Comviva**
Douglas	Kinloch	**Inside Secure**
Henrik	Karlsson	**Ericsson**
Bastien	Latge	**Inside Secure**
Andre	Zoelch	**PostFinance**
Ira	McDonald	**Trusted Computer Group**
Teresa	Mesquita	**SIBS**
Camhi	Michel-Ange	**Worldline**
Tero	Mononen	**Giesecke-Devrient**
Ciara	Myers	**AIB**
Philippe	Roy	**Danske Bank**
Stephen	Sherwin	**AIB**
Ville	Sointu	**Ericsson**
Rajasekaran	Soruban	**Mahindra Comviva**

This document provides an overview of the results of the biometrics survey conducted by Mobey Forum.

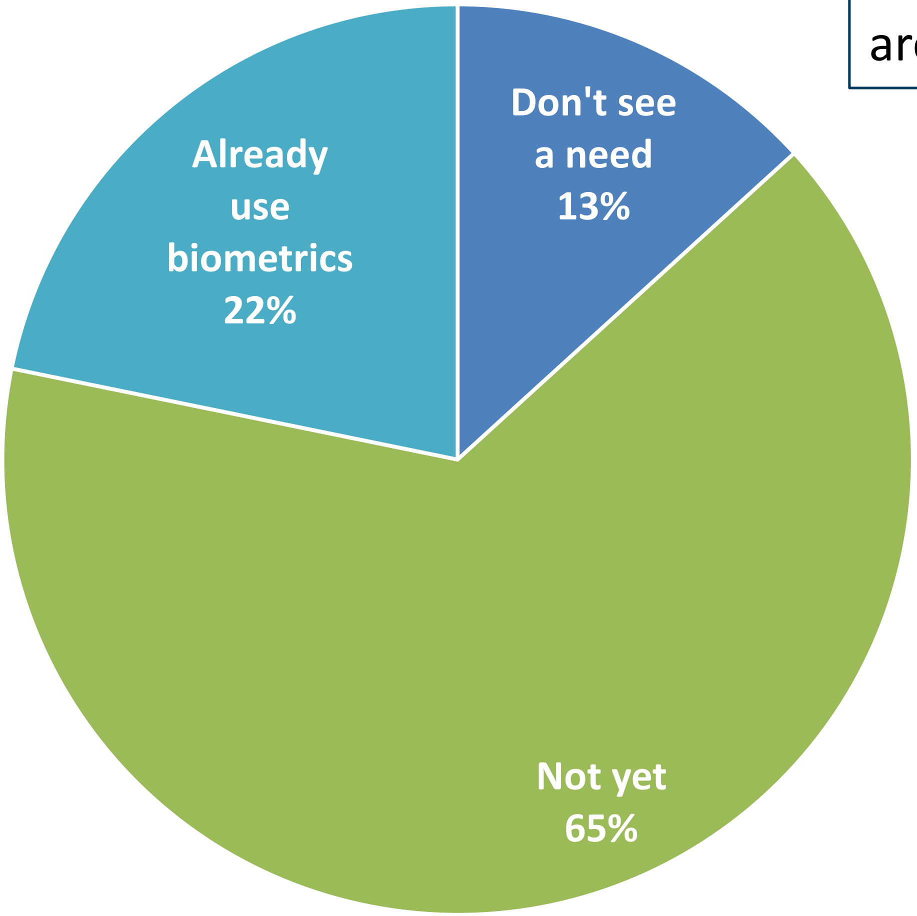
- 235 respondents of whom
  - 59% were from banks and financial institutions
  - 32% were from solution providers
- Survey responses during the first half of 2015
- Geographic area: Europe, North America, Middle East

Q: What type of company do you represent?



The majority of the survey respondents represent
banks (44%) or
financial institutions (15%),
together 59%.

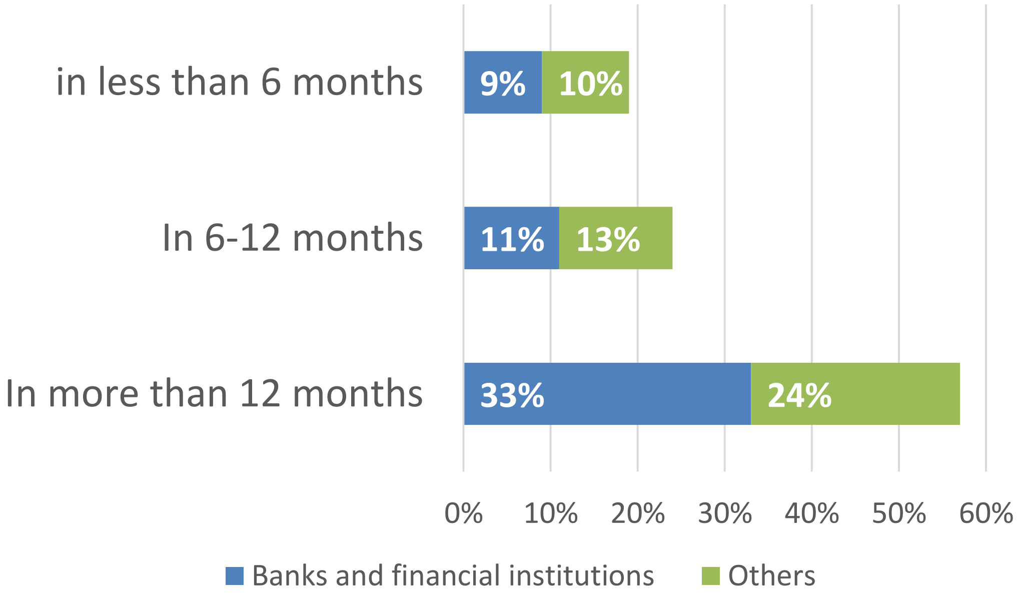
Q: Do you offer biometric authentication for mobile financial services to your customers today?



Out of 235 respondents
... Only 22% offer biometrics

Most of the respondents do not offer biometric authentication for mobile financial services yet, but are planning to do so in the future.

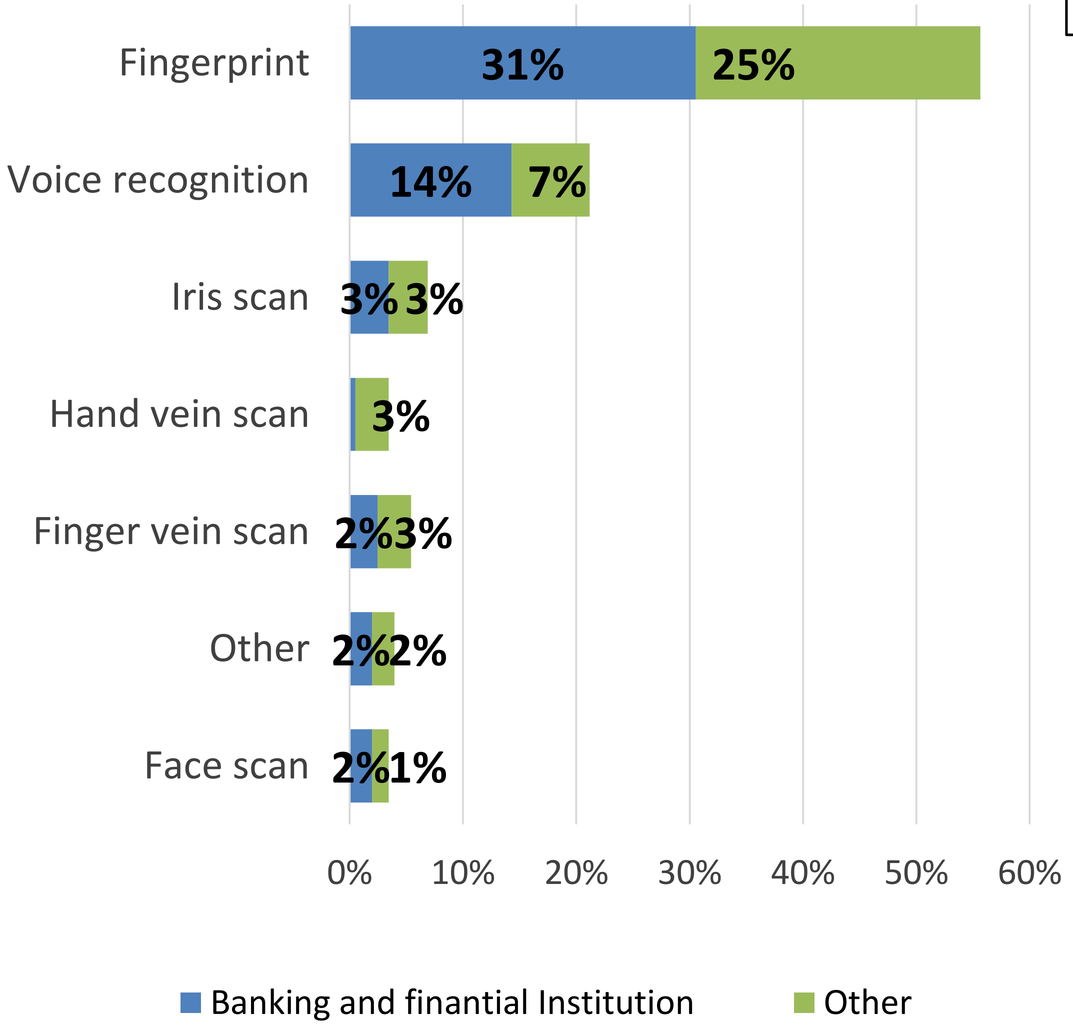
Q: How soon are you planning to launch biometric services?



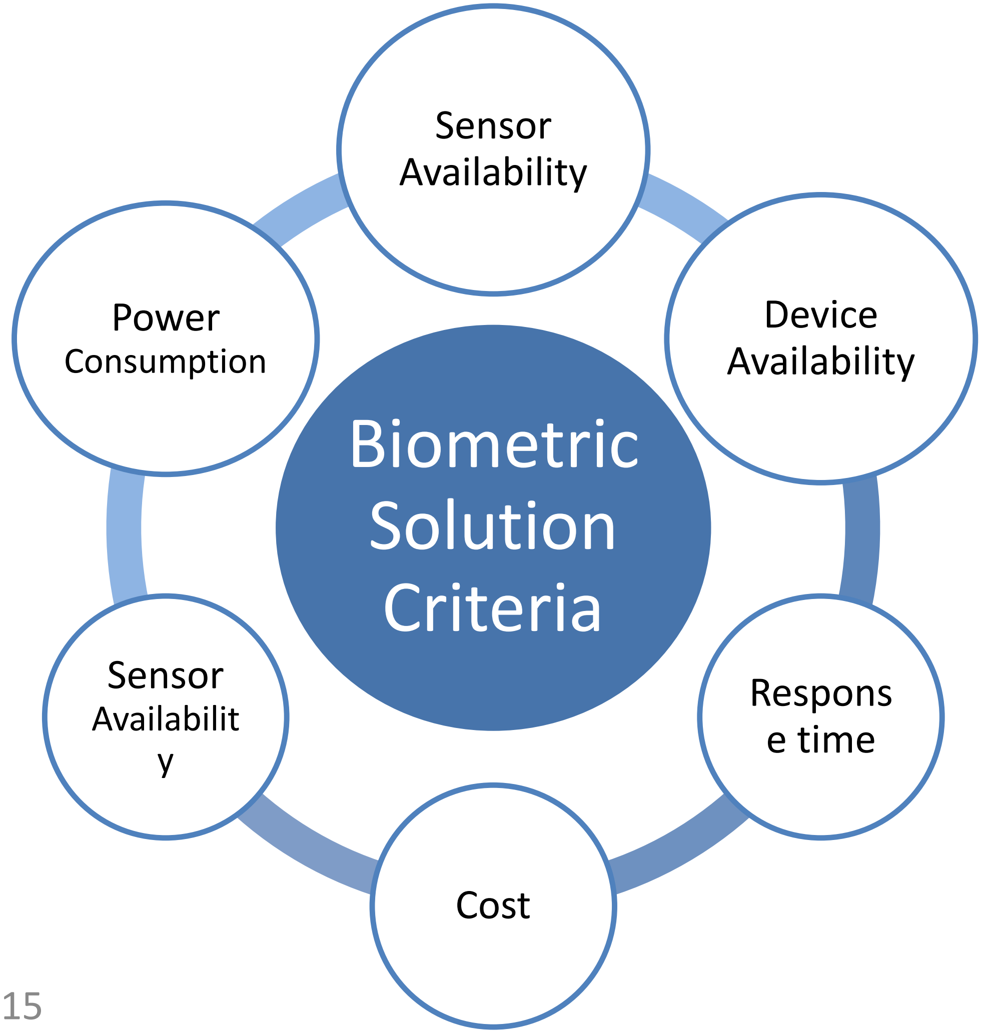
mobey forum

All Respondents

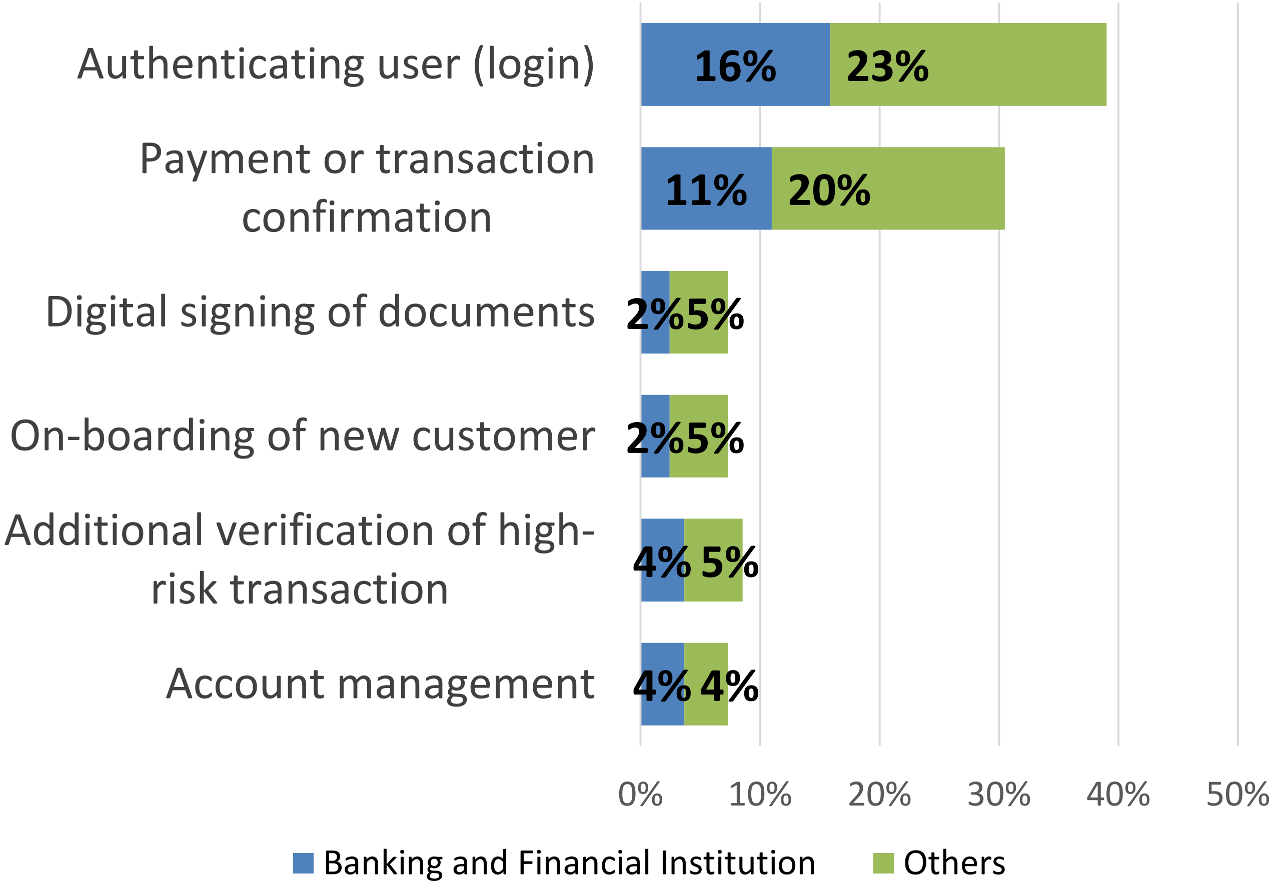
Q: What kind of technology are you planning to use?



Fingerprint is the dominant technology, also for financial institutions. It fulfils most of the solution criteria described below.



Q: What type of services do you use biometrics for OR are looking to offer in the near future?



Authenticating the user at the login and payment or transaction confirmation are the biggest use cases for biometrics in mobile financial serivces.

Other possible use cases mentioned:

- Identification of the customer calling
- Risk assessment
- Wallet authentication

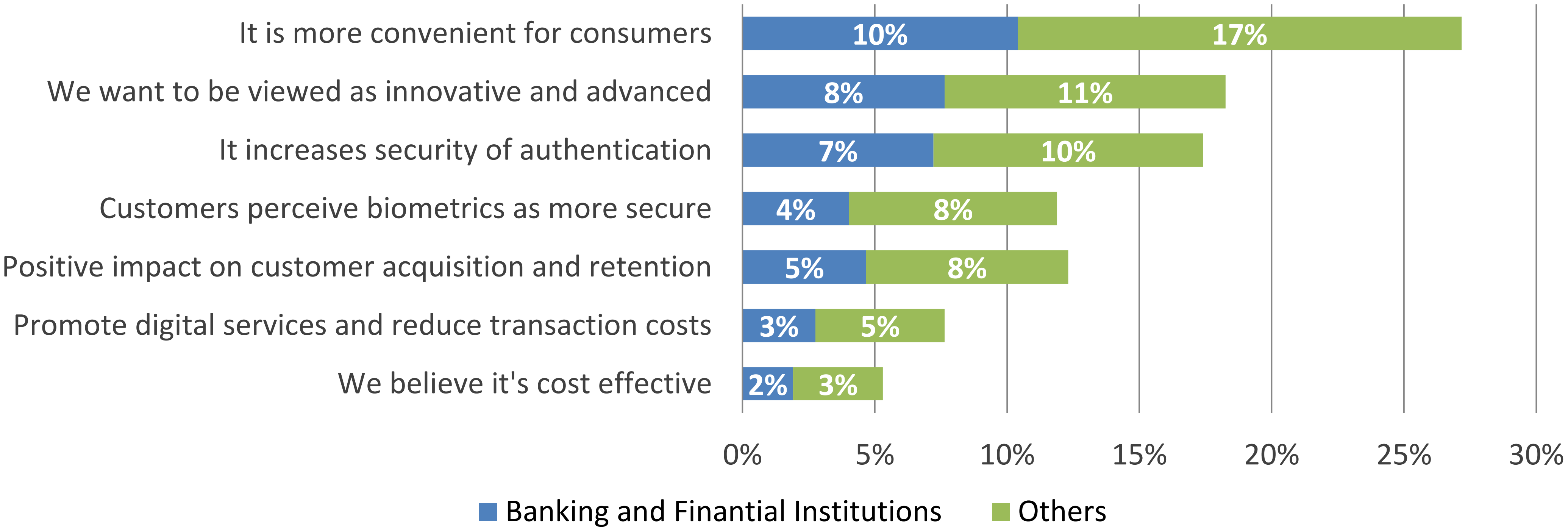
mobey forum

All Respondents

The main drivers for the adoption biometrics by financial institutions:

1. Convenience, innovativeness, technologically advanced.
2. Increase in security or perception of security.
3. Positive impact on customer retention and acquisition.

Q: Why is biometrics interesting for you company?

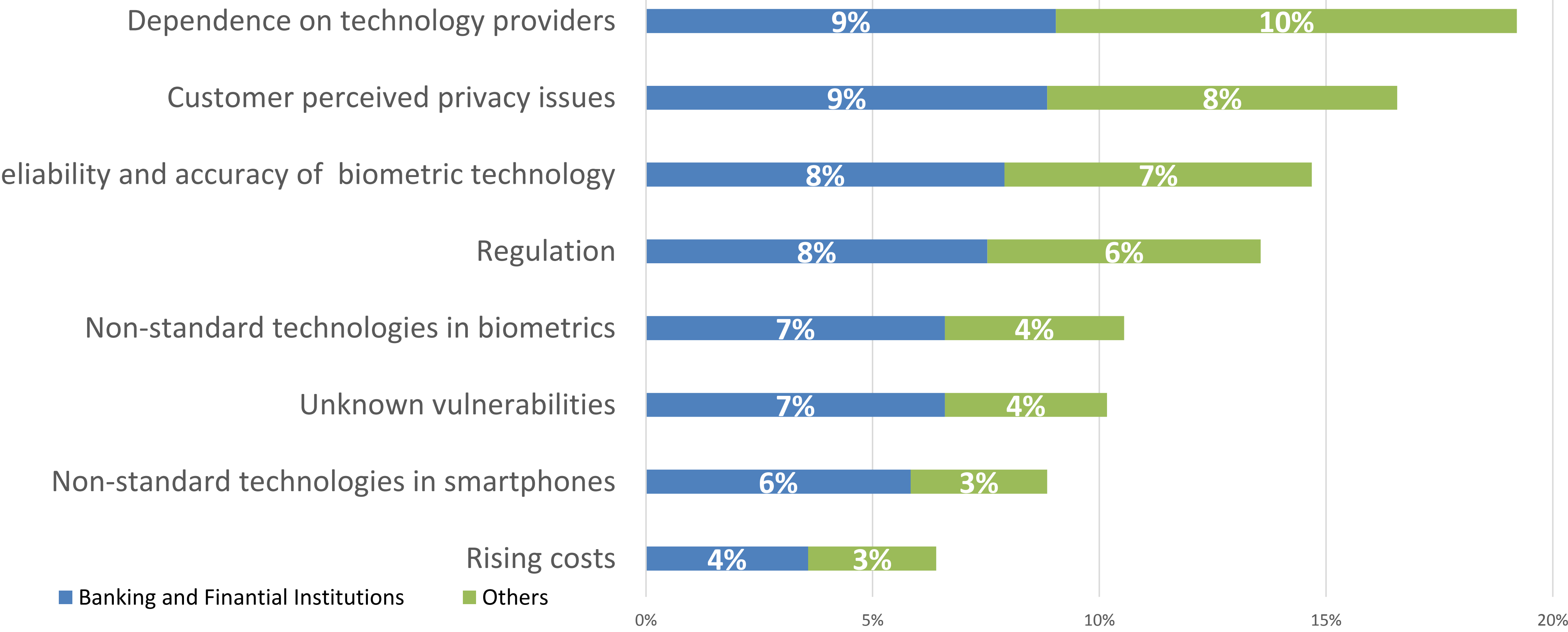


All Respondents

The biggest obstacles for financial institutions in adpting biometrics

1. Dependence on technology providers, including handset vendors
2. Customers' perceived privacy issues
3. Reliability and accuracy of biometric technology
4. Regulation and its uncertainty

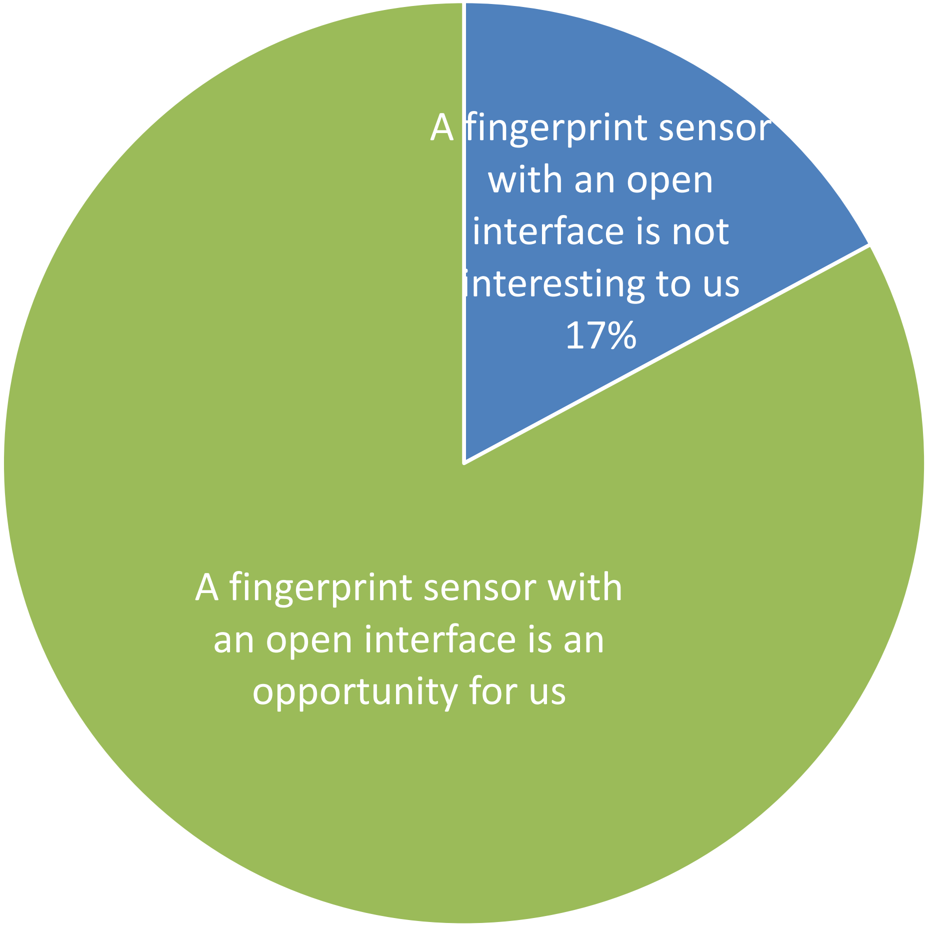
Q: What do you think are the biggest obstacles in adopting biometric authentication? (you can tick many)



Banks only

Q: Handset manufacturers have been integrating fingerprint sensor in mobile devices. Some of the fingerprint sensors have **an open interface,** where the authentication data can be controlled by the bank or a provider chosen by the bank.

How do you see this development?



An open interface is perceived as better option for banks.

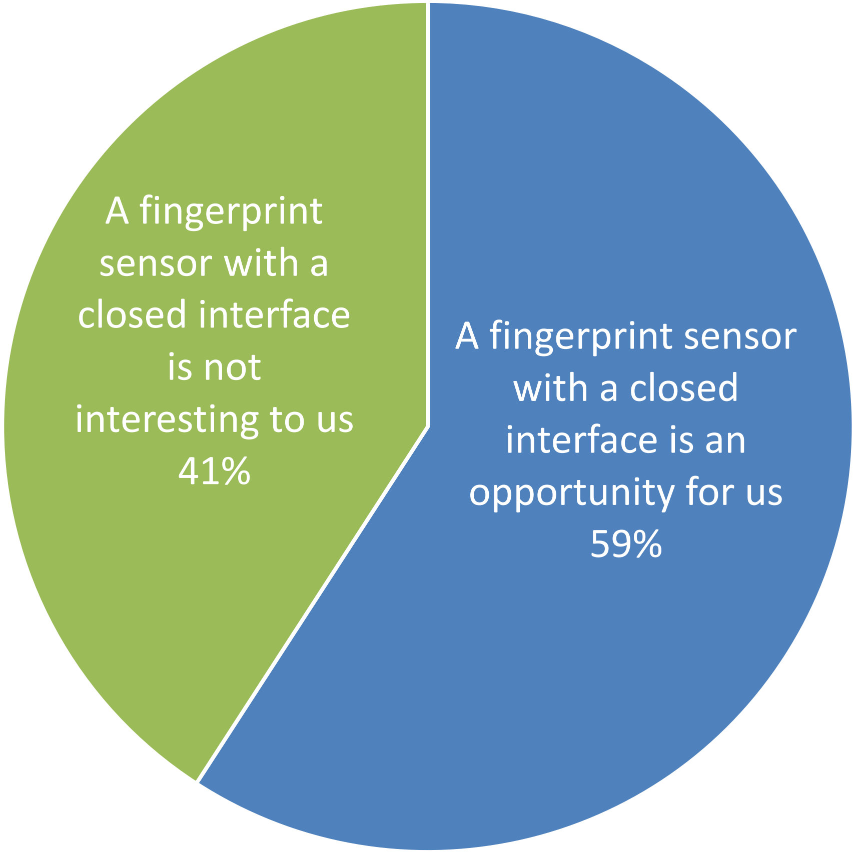
As expected, open interface is significantly less controversial than a closed interface.

The data can be stored and owned by bank and security-related paradigms are within controllable limits.

mobey forum

Banks only

Q: Handset manufacturers have been integrating fingerprint sensor in mobile devices. Some of the fingerprint sensors have **a closed interface**, where the authentication data controlled by the handset manufacturer. An example of this is Apple's Touch ID.
How do you see this development?



From a bank's perspective, even when the interface is closed, a fingerprint sensor can reach out to new customers. It can help diminish customer complaints about signing into a bank's services.

Banks say:
"We have customers asking why they can't use Apple ID to log in to their mobile banking. It's an opportunity to say we are using cool stuff: As a result, we get positive feedback and increased take-up."

"People don't care about financial privacy because they use it [AppleID] anyway."

mobey forum

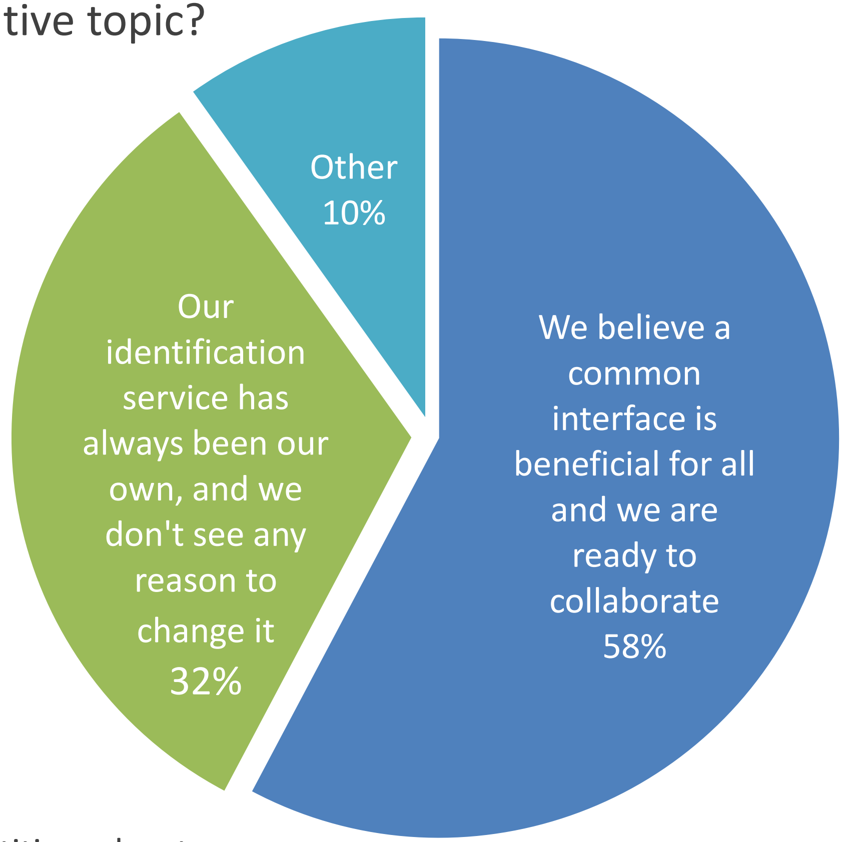
Banks only

Q: When biometrics is used for identification, would you as a bank see this more as an inter-bank topic (similar interfaces to all banks) or is this a competitive topic?

58 % of banks are willing to collaborate in biometric authentication (one identity for many services).

Mobey Forum believes this is the future – all successful financial solutions need to be easy and convenient.

Also ECB regulation (SecuRePay) accepts this type of collaboration.



OTHER comments in the survey included:

- Authentication will and should eventually be common, but now is a competitive advantage.
- Mechanism can be set as a standard, but how this will be used should be competitive topic.
- Not all banks will see this as an opportunity, therefore it is likely to be an issue we have to deal with ourselves. However, we support standards.
- Both options are possible, depending on market and tactics – difficult to say in my bank at the moment.
- It's for sure both. It's common interest regarding security and competitive on commodity/perception of the customers
- It depends on what will be standardized and on what level – Banks should collaborate on this.

Conclusions

- The **usage of biometrics** in financial services **on the rise**, and more banks are looking into the opportunities offered by it.
- Fingerprint is the **dominant technology** as it fulfills most of the solution criteria for mobile biometrics.
- Most banks see **figerprint sensors integrated in handsets** by manufacturers as **an opportunity**, especially when the interface is open.
- **Authentication and payment or transaction confirmation are the most often considered use cases** for biometrics in mobile financial serivces.
- Main drivers for selecting to use biometrics are **1) being viewed as innovative, 2) increased security and 3) customer retention.**
- Main obstacles for banks in adopting biometrics are the **dependence on technology providers, perceived privacy issues, reliability of the technology and the uncertainty in regulation.**
- Biometrics are seen as a **point of collaboration for banks:** the majority of banks believe that a **common interface is beneficial for a all** and are willing to collaborate to create such interface.

Further Discussion points on risks regarding the use of biometrics in financial services

Below is a list of some of the key issues that have come up in the workgroup discussions. The banks and the technology experts will continue to analyse these potential obstacles for the successful use of biometrics in financial services.

1. **Reliability**. Existing equipment does not guarantee 100% effectiveness. As a consequence, most biometric identification systems are combined with an additional mechanism (PIN, asking date of birth, NFC, etc.) to achieve authentication in 2 or 3 steps.

2. **Non-standard technologies**. Each device manufacturer uses its own algorithms, biometric scanners and software applications and there is a lack standardization.

3. **Multimodal systems**. There is a trend to combine multimodal systems to mitigate the lack of the different systems.

Further Discussion points on risks regarding the use of biometrics in financial services

4. **Attacks**. By impostors who pretend to be authorized personnel.
    - *Administrative attacks*. Attacks that use the incorrect administration of the biometric system.
    - *Unsafe Infrastructure*. Attacks that try to manipulate the biometric infrastructure (e.g. software, hardware, communications, etc.).
    - *Identity theft*.
5. **Reluctance**. Some users show some reluctance to use biometrics.

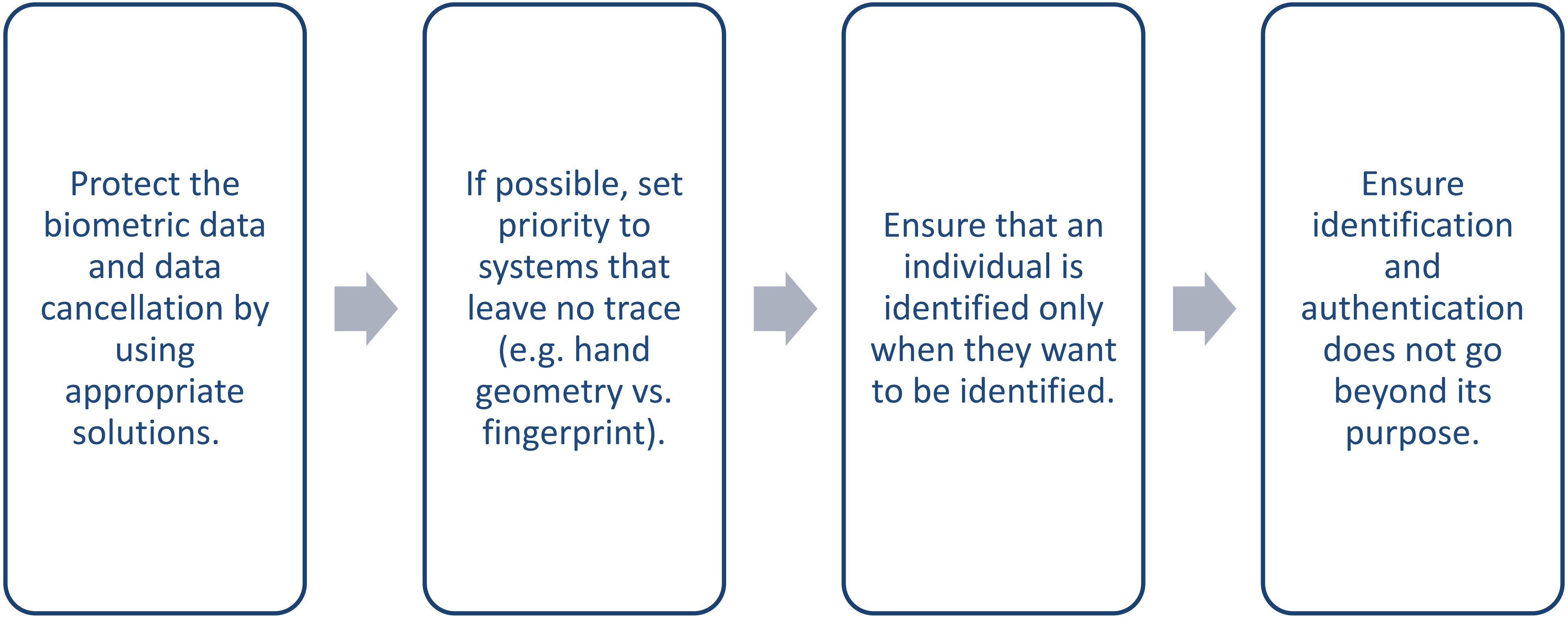
6. **Personal data**.

    The biometric data cannot be changed and is not exclusive to one system. Users do not have the ability to change biometrics as they can passwords.

7. **Privacy and data protection**.

    Concern for a loss of personal freedom. For example, a company acquires the biometric data of an individual. The company has the data forever since it cannot be changed and the data can be used to detect features for which the user hasn't given consent (e.g. identifying genetic diseases). It an optimal situation there would be a combination of centralized and decentralized storage of data to ensure that the date cannot be misused.

How to mitigate the risks?



Protect the biometric data and data cancellation by using appropriate solutions.

If possible, set priority to systems that leave no trace (e.g. hand geometry vs. fingerprint).

Ensure that an individual is identified only when they want to be identified.

Ensure identification and authentication does not go beyond its purpose.

Mobey Forum cordially thanks all the participants of its Biometrics Workgroup; its chairpersons as well as all the industry partners who have given their valuable time to answer this survey.

The work continues –
if you would like to be a part of it,
please contact
mobeyforum@mobeyforum.org
www.mobeyforum.org

mobey forum