thalesgroup.com

THALES

Thales: building trust in mobile apps

The consumer perspective

Contents

Foreword

Today we are witnessing a convergence of industries in the mobile world as well as the undeniable influence of mobile on every aspect of our lives. The rise of handsets, smartphones, tablets, and now wearables has driven new means of communicating. It has also influenced how we buy products, bank, interact with brands, and even created an entire industry in the app economy. Whenever we appreciate an advert on television, our natural instinct is to reach for our smartphone or tablet in response. If we want to get in touch with a friend, it is our mobiles we turn to. Governments, too, are capitalizing on the mobile revolution, illustrated by the emergence of mobile ID initiatives, such as mobile driving licenses in the USA. Our mobile devices have quickly become the primary way we engage with the world.

There is however a threat in this new mobile-centric world, and it comes in the constantly evolving shape of cyber-attackers. Hackers know a successful data breach could net them financial details, social network logins, mobile network account details and perhaps enough to commit identity fraud. This threat is especially pertinent now as app development is rising quickly; **90% of companies will increase mobile app investment by the end of this year**[1]. And it's not just large businesses - in the US, 47 percent of small businesses will either have or be planning their own app by the end of 2017[2]. More apps mean more opportunities for cyber-attackers.

There's also been an increase in app usage, further increasing the number of opportunities for attack. Consumers are spending more time with their devices than ever before. End users will spend over three hours a day on their smartphones this year[3], and 87 percent of this time will be spent using apps.

Attackers are increasingly aware of this; they are well-organized and skilled at spreading malware, exploiting non-official app stores, infecting emails, distributing fraudulent SMS messages and infiltrating browsers to achieve their aims. App providers need to adopt a vigilant attitude towards these threats and help consumers feel safe with genuine solutions that protect against vulnerabilities.
In line with this, enterprises need to take strong action to protect their brands on mobile as malware deployed by 'lookalike' apps is a growing problem. If apps and services are copied, trust can be quickly eroded if consumers are scammed into using non-official versions.
It is a problem we need to address by finding a security solution that works for everyone in a convenient way, and that does not intrude on the user-experience. In order to do that, it is crucial we understand what consumers need and expect from their mobile devices and their perceptions of mobile security.

With this in mind, we commissioned a study of over 1,300 adult smartphone users across six markets: Brazil, UK, South Africa, Singapore, the Netherlands and the U.S., asking people about their mobile behavior and security expectations. We wanted to discover how consumer expectations would have an impact on those providing applications and infrastructure for mobile applications and services; be they banks, government, MNOs and any other large enterprises which develop apps for end users.

In this report, we use these insights to offer a series of recommendations to help build greater trust in the mobile ecosystem and deliver a secure and convenient experience for users.

> **End users will spend over three hours a day on their smartphones this year[3].**

1: 90% Of Companies Will Increase Mobile App Investment In 2016, ARC
2: Mobile Apps and Small Business in 2016: A Survey, Clutch
3: Growth to slow to single-digit pace starting in 2016, eMarketer

Executive Summary

The results of the survey, conducted in different countries and continents, revealed several key insights into the expectations of end users with regard to app usage and mobile security. Overall, the insights revealed similar trends in attitude that transcend regional/cultural differences. In the summary below, we've listed some of the most significant findings.

- When it comes to the attributes of paid apps, end users value reliability and security most (80%). Convenience and speed also ranks highly (second with 48% of respondents valuing it among the top two most important attributes)
- End users are split in their expectations of where the burden of responsibility should lie for app security – most of them believe that app providers are best placed to protect smartphone apps
- 60% expect security on their smartphones to be easy and frictionless, with the use of PIN, fingerprint, password, or pattern authentication once and then have total access to all apps on their phone
- 70% would want to use digital identity documents on their smartphone, such as passport or national ID card, if they knew all apps on their phones were 100% protected
- 66% of end users say they would perform more transactions if they knew mobile security was on board with their devices

With these findings taken into consideration, we've made a range of recommendations for the mobile app ecosystem to increase security and build trust with end users. These include:

- The use of (Software Development Kits) SDKs, so that apps can become self-reliant and deal with the dynamic nature of malwares. The use of SDKs gives apps the much-needed ability to defend themselves while in the field, detect unsecure environment and react accordingly. SDKs also better protect users as they enable strong authentication
- User experience needs to become as centric to the design process of mobile apps as possible. This includes embracing the "psychology of security" together with biometry, which plays a key role in a user's experience and ensures strong authentication
- In conjunction with SDKs, flexible risk management systems should be adopted, which can respond to new situations and implement adaptable security policies while the apps are used in the field
- The mobile app ecosystem needs to adopt a layered approach to protection to ensure security levels can adapt in line with what is at stake. For instance, this approach can be used to counteract the growing levels of sophistication from hackers

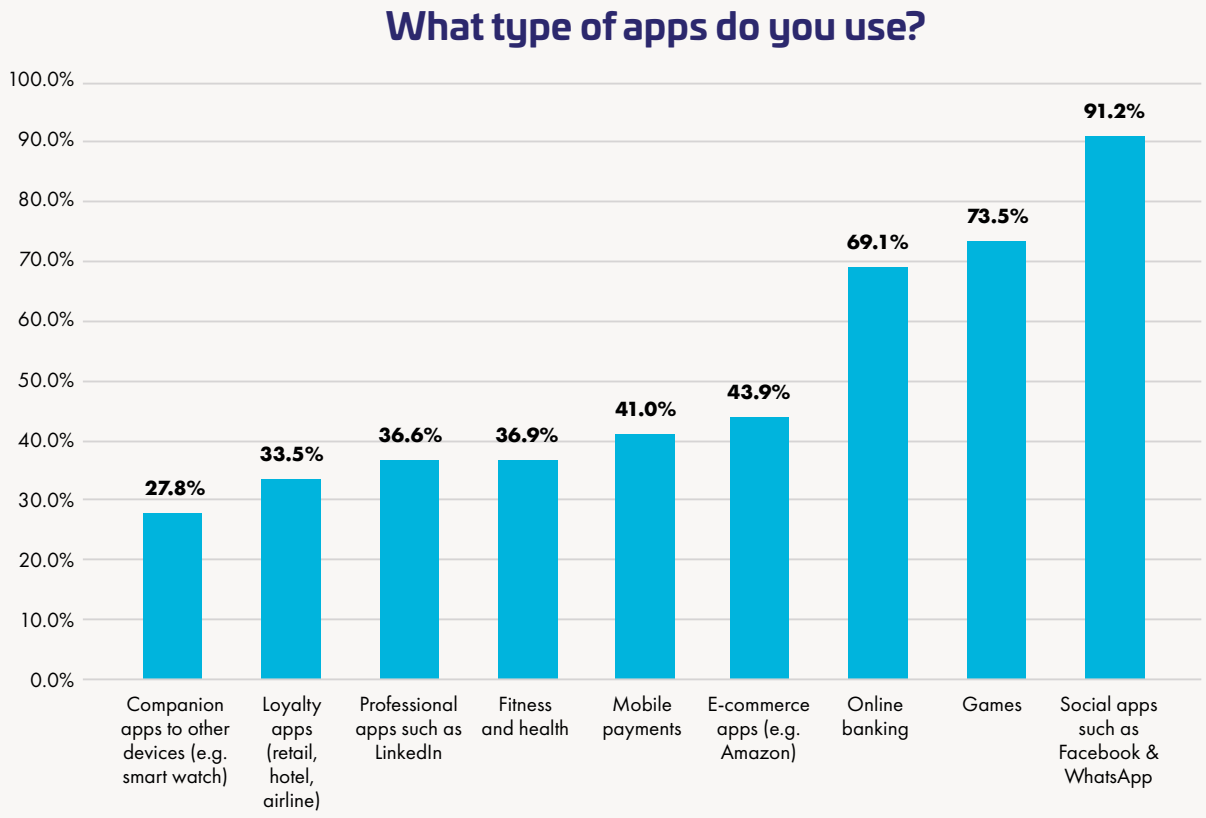
PART 1: MOBILE SECURITY SURVEY

The survey was designed to gain insight into the minds of consumers; how they approach security, and what they expect from the apps they use. The results indicate the direction companies may consider when they come to building apps of their own.

Research methodology:

An independent consumer survey of 1,300 adult smartphone users in Brazil, the Netherlands, South Africa, Singapore, the UK and the U.S. was carried out by Smart Survey on behalf of Thales in July 2016.

Fig 1: Most popular apps



Unsurprisingly, social apps such as Facebook and WhatsApp top the list in all countries in terms of popularity. Looking closely at the results, it's been intriguing to see how the UK, one of the most saturated smartphone markets, has the lowest percentage of social app users (83 percent), while Brazil has the highest (97 percent). It is clear Brazilian consumers attach great importance to using their smartphone – coming first in app usage for all categories.

Games and banking are the next most popular categories, followed by shopping and payments apps in fourth and fifth.

Unsurprisingly, social apps such as Facebook and WhatsApp top the list in all countries in terms of popularity.

This snapshot into how the modern global consumer uses their smartphone highlights the important role security needs to play. Banking and payment apps are used more than ever before now by smartphones; these apps are prime targets for hackers. Consequently, to protect their consumers, industries developing apps must take this into consideration and integrate security into them.

> Banking and payment apps are used more than ever before now by smartphones; these apps are prime targets for hackers.

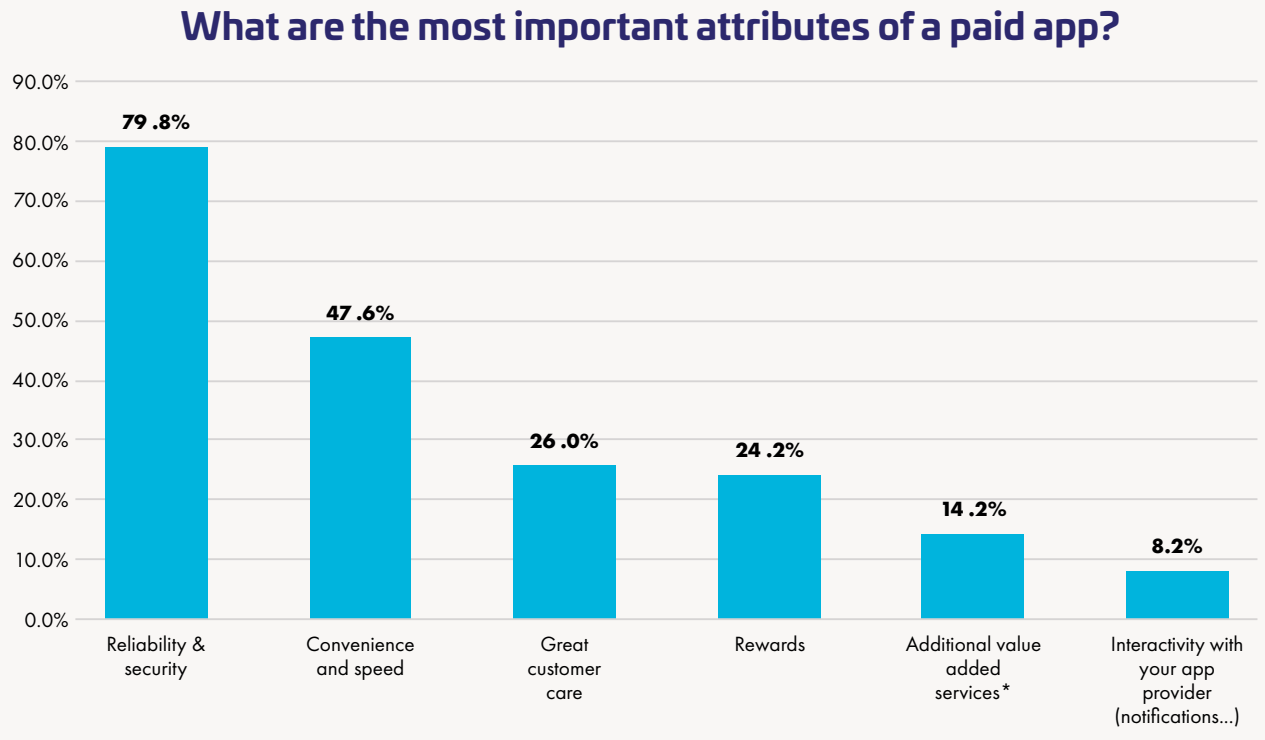
It is encouraging that the vast majority of end users (80 percent) value reliability and security above other attributes. Clearly the message is getting through in some ways; consumers understand they cannot afford a mobile experience without security.

Convenience and speed are also very important, valued by just under half (48 percent) of respondents. This shows that while security is vital, people expect a frictionless experience. Industries and those in government designing apps for their own users should take note of this and ensure their software is lean, runs quickly, but is also fundamentally secure.

Customer care narrowly pips rewards as the third most important attribute. And this is only because of regional differences. 42 percent of Brazilians see great customer care as a critical attribute (in addition to reliability and security), by far the highest of any country, and yet only eight percent of all respondents value rewards. If Brazil is omitted then rewards rises to third in importance, suggesting that for the majority of mobile users, this is more valued than access to app support.

> It is encouraging that the vast majority of end users (80 percent) value reliability and security above other attributes.

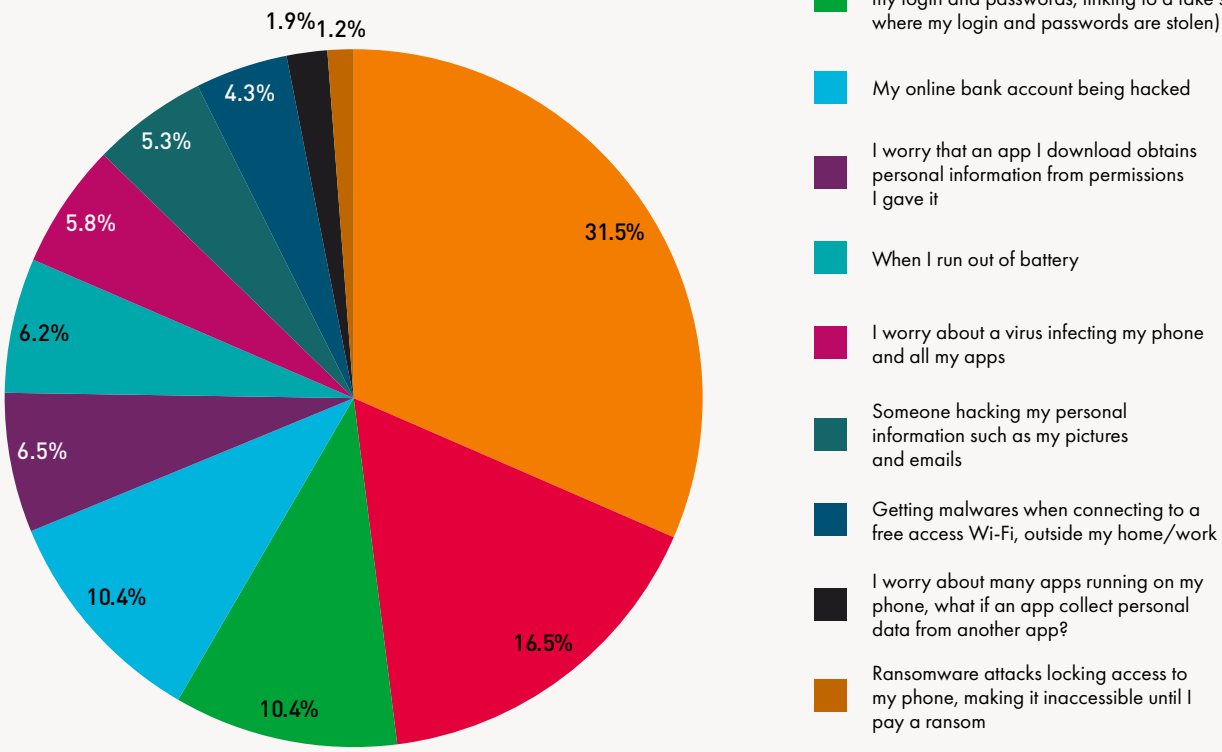
Fig 2: App attributes



*Additional value added services (services updates, personal data updates etc.)

Fig 3: Smartphone vulnerabilities

What do you fear the most regarding your smart phone or apps?



The top four smartphone concerns paint an intriguing picture – we can see fear of losing data, fraud, phishing and viruses are in the minds of many. At a first glance, it seems consumers are taking threats seriously. When we look more closely, we see that there is still an education gap.

Only 4.3 percent of consumers are most concerned about the possibility of malware getting onto their mobile if they connect to an open Wi-Fi network. And though there are numerous attacks that can occur on unsecure networks, the public still do not appear to be overly concerned. Fear of ransomware attacks locking access to a phone was even lower at only 1.2 percent of respondents.

Thanks to awareness-raising campaigns, the public are well-aware of phishing and fraud attacks. It is the more sophisticated attacks that now need to be addressed. Mobile industry bodies need to show end-users how attacks like the man-in-the-middle attack work and the steps consumers should take to protect themselves. The first step is recognizing them as a legitimate threat.

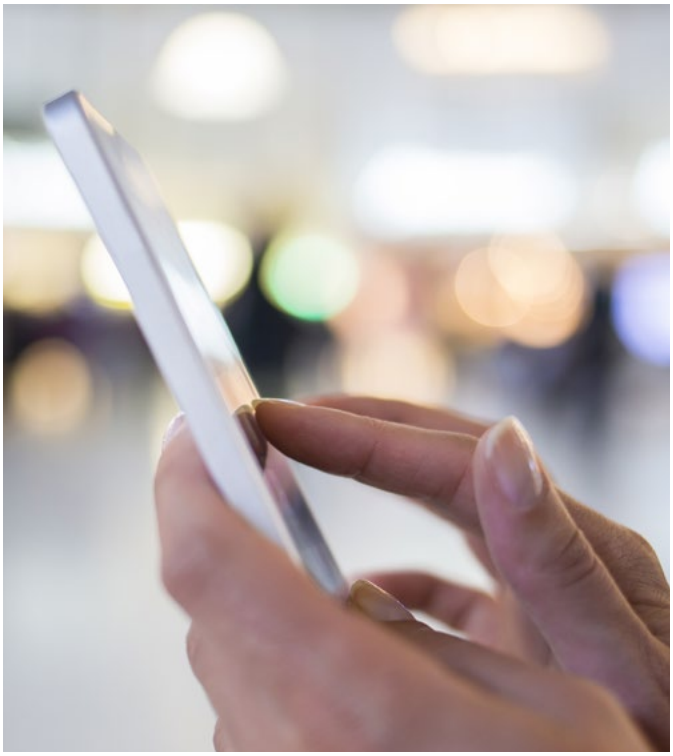
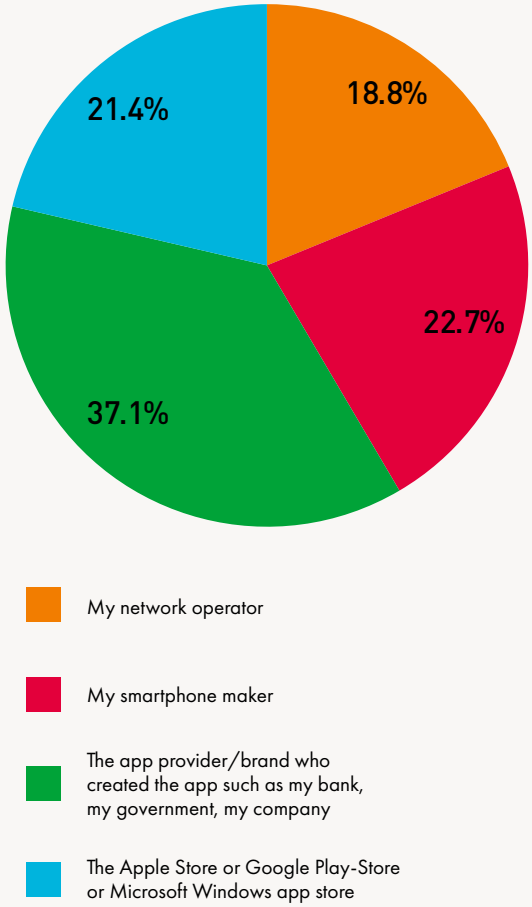


Fig 4: App protection

Who do you think is best positioned to protect the apps in your smartphone?



Who ultimately is best placed to safeguard a user's security has been a debate for years. Many within the industry would suggest it is the app stores' responsibility to police the software available, or the smartphone maker who controls the OS. However, when it comes to the general public, the results are pretty evenly split. Interestingly, many place the greatest onus on the app provider (such as bank, corporate enterprise, or government) itself – suggesting that if their app's security was compromised, the brand who made it would take the greatest reputation hit.

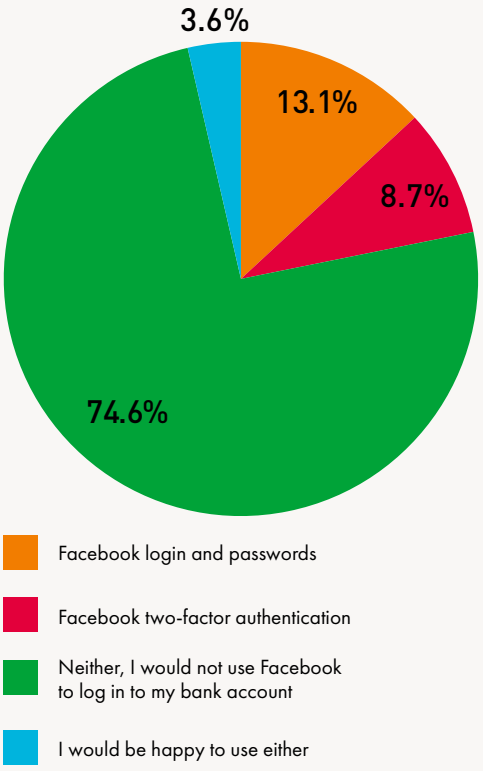
While it is true that ultimately security lies with the app provider, once a party wants to create malicious software or has discovered a vulnerability in an app, it is up to others to ensure the threat is discovered, and any damage mitigated. As is clear, each stakeholder bears responsibility for any serious security breach; the stores must remove offending apps, smartphone makers must patch any exploits in their OS, app providers need to update their software, and MNOs need to be on-hand to push out patches over the air quickly.

There are also some eye-catching regional contrasts, albeit familiar as Brazil was the outlier again. Those in the UK think the mobile operator is best placed to protect the end-user from third-party apps, while in Brazil it is the job of the app store. Those in South Africa, Singapore, the Netherlands and the United States all think the app provider must ensure their apps are secure.

Many place the greatest onus on the app provider (such as bank, corporate enterprise, or government) itself – suggesting that if their app's security was compromised, the brand who made it would take the greatest reputation hit.

Fig 5: Facebook and banking

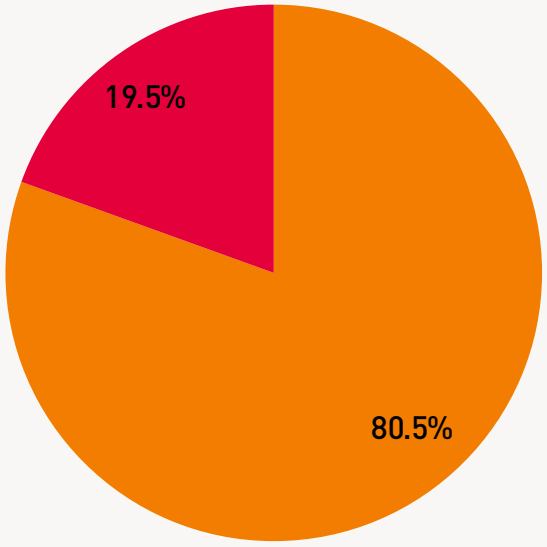
Would you log on to your bank account using Facebook login and passwords, or Facebook two-factor authentication?



The results suggest that our respondents recognized there is too much risk involved with pairing social media credentials with something as important as your bank account.

Fig 6: Security perception

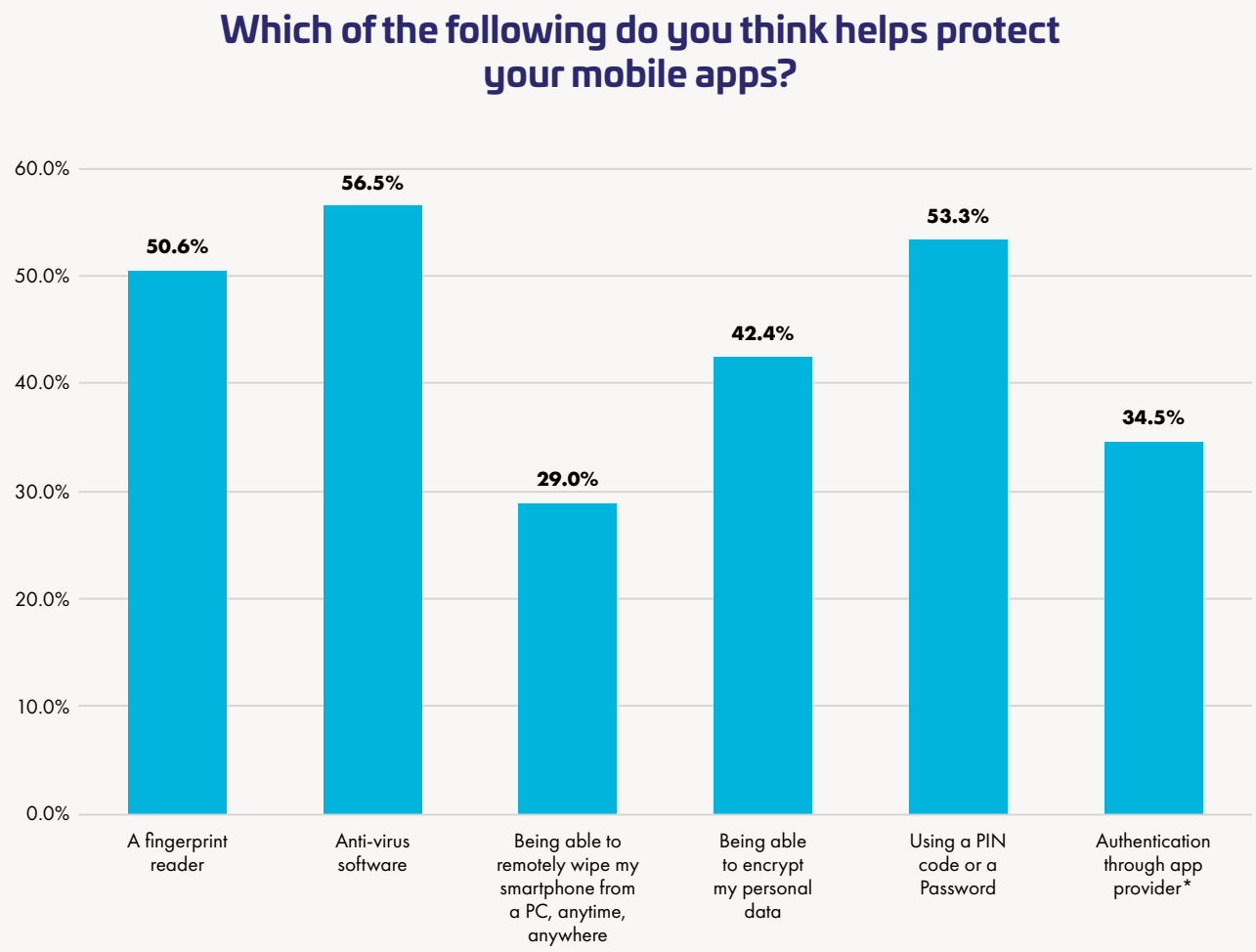
Which of the following do you agree with most?



It seems when it comes to security, the saying "out of sight, out of mind" does not apply. People want to know they are protected, even if they have an app installed. It illustrates the psychology of security as, unsurprisingly, four out of five users feel more confident if a security app is visually displayed on the smartphone screen. This suggests that as long as users recognize a form of security or feel they are in a safe digital environment, they feel more secure, which will encourage application uptake and usage. This is an important lesson for industries and governments to learn, to establish how they can incorporate this feeling of security into their applications.

In the UK and U.S., where the app ecosystem is very mature, we note that respondents have the most faith in app providers. A quarter have enough confidence in the security expertise of their providers that they do not need a visual cue that they are secure. This means that app providers may want to vary their apps to meet the needs of end-users in individual markets.

Fig 7: What makes an app secure



* The app provider requires a user to authenticate themselves with a secret phrase if the use of the phone is unusual (unusual location, unusual transactions...) via SMS, email, or a phone call

When asked about general mobile security approaches (covering both authentication and security techniques), consumers are broadly aware of how they can be protected. It's encouraging to see how consumers positively value such a range of security solutions.

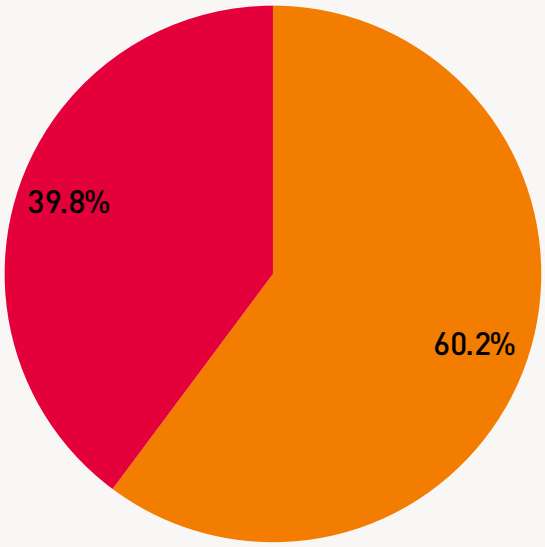
The show of enthusiasm for fingerprint biometric authentication is also worth consideration, if only as a stepping stone to future development in the area. Apple revolutionized security when it debuted TouchID in 2013, an innovation that is now a feature of almost all smartphones.

It could be argued that app providers and the wider mobile industry need to do more to convince users of the need for vigilance when it comes to mobile. Only 53% of people think a PIN or password protects them, only just over a third value two-factor authentication, and only 42 percent feel encryption would help is surprising. Perhaps people falsely assume that their phones are safe from malware and intrusion, a false sense of security that could stem from the historical safety of feature phones. Furthermore, it's worth noting how the results show that users would consider multiple methods of protecting their apps; not a single method, but different methods working alongside each other.

It could be argued that app providers and the wider mobile industry need to do more to convince users of the need for vigilance when it comes to mobile.

Fig 8: Two approaches to app security

Which of these two statements best describes what you would like to experience when using your mobile apps?



The response to this question reiterates the importance of building frictionless security solutions which do not impact upon the user experience. Overall, a strong majority of respondents (60 percent) prefer one-time authentication. It's clear authentication methods will continue to play a role in the quality of mobile experience.

Consequently, app providers face an important challenge if they want to change the user journey. They will have to find a way to provide secure authentication in a way that isn't disruptive or perceived to be inconvenient. Otherwise people will just sign in, and click the 'remember me' tick-box to avoid the hassle, or avoid the digital route entirely in favor of a costlier customer experience touchpoint, like a face-to-face visit or call to the call center.

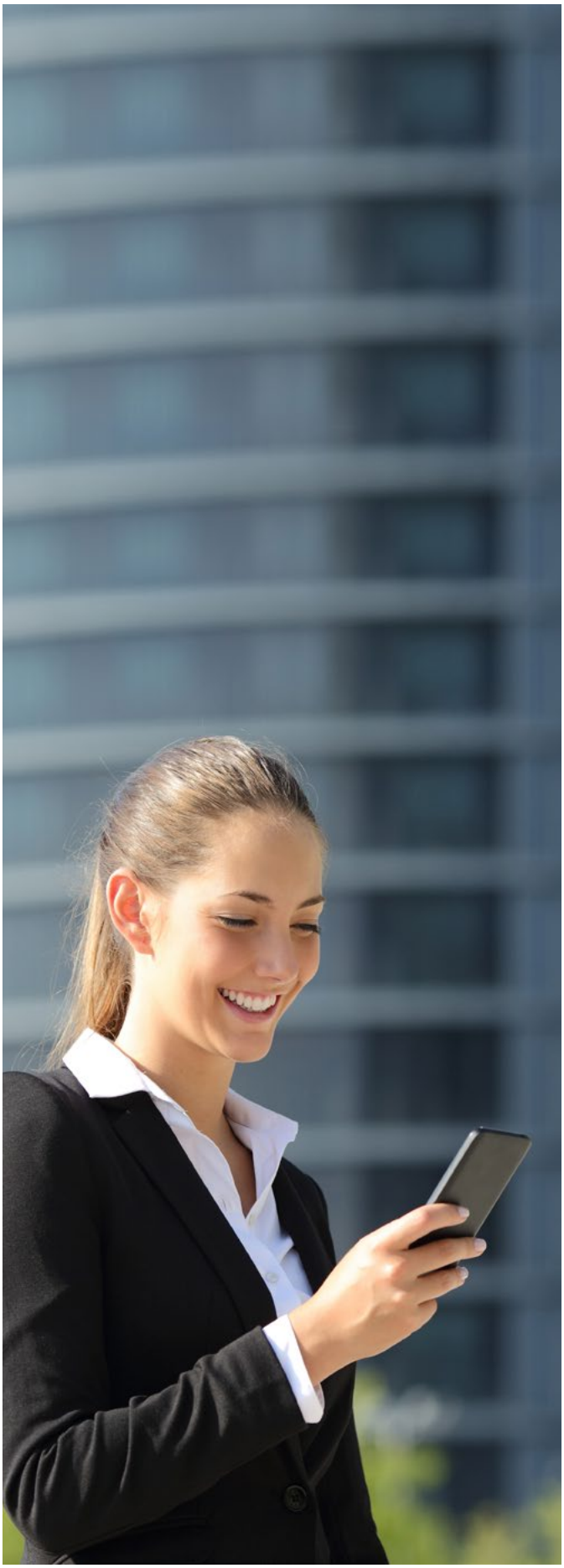
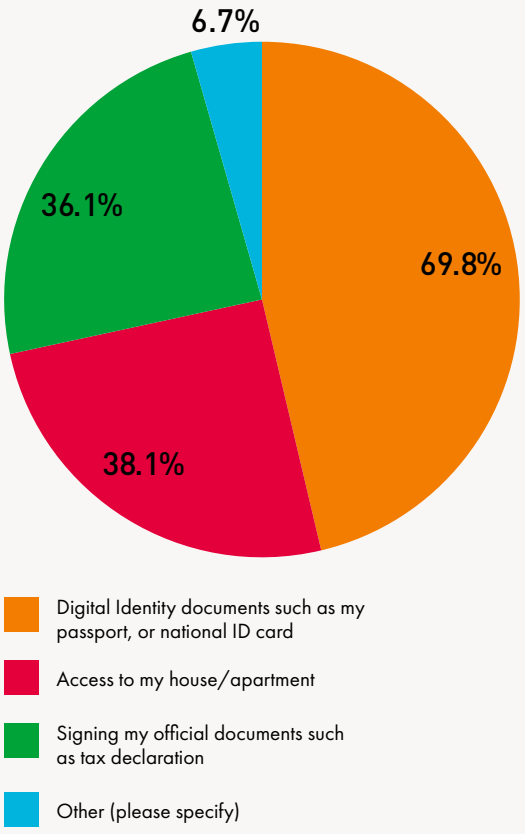


Fig 9: If security is guaranteed, what would you like your smartphone to do?

If all the apps in your phone are 100% protected, what new app(s) would you like to have in your smart phone?



It is fascinating to see what happens when you can guarantee security. People open their minds, and are much more willing to embrace new technologies. These results suggest once security obstacles are overcome, mobile consumers are more enthusiastic about using digital identity documents, such as a passport or ID cards on their smartphones.

This was particularly high in Brazil (84 percent) and South Africa (76 percent), and should be welcomed by their governments. Technology when deployed correctly, can bring significant benefits to a country, and it is clear that these countries are more than ready for eGoverment services. This could have a significant effect in enfranchising those that cannot partake in many services due to poor physical infrastructure. Health, voting, education, and identity services are just a few areas that could all be revolutionized by embracing the power of mobile.

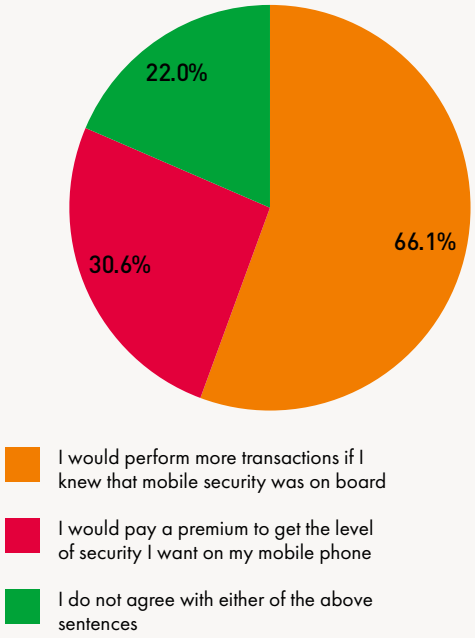
The Internet of Things also gets a boost, with a notable appetite for access to a house/apartment via a mobile app. Just over four in ten in Singapore (44 percent) and the U.S. (43 percent) are ready for this technology – something that should be embraced by smart home vendors and solutions providers. Still with the smart home being pushed by major technology players, the future looks bright given most consumer IoT products are still in their first iterations.

In addition, it's also worth noting how Brazil by far is the nation most willing to embrace access to houses/apartments through their smart phones - over half (55.5%) would use this form of access if security were guaranteed.

It is also clear that consumers would be more willing to perform transactions via their phone if security was guaranteed, and that almost a third of consumers are willing to pay a premium to get the level of security they want as seen below:

Fig 10: Would you perform more transactions if security was guaranteed?

Do you agree with either of the two sentences?



PART 2: RECOMMENDATIONS TO BUILD TRUST IN THE MOBILE ECOSYSTEM

In the first part of this report, we learnt that consumers want and expect a secure app ecosystem, with their experience to be frictionless.

- For those organizations who have developed or are planning to release an app, there are a series of steps they can take to build trust with their end-users. Apps must be securely designed to coexist in an environment where there are many others from third-parties they do not control: they need to be able to react and defend themselves, while on the field
- Layers of protection should be implemented, with the psychology of security in mind, to make the user feel secure. This can range from visible icons to show everything is operating as intended, to login procedures like biometric authentication such as fingerprint, facial recognition, iris scanning
- App providers must gauge their audience and the purpose of their app. In some instances, connecting a user account with a social network may be acceptable, but many in others—such as banking or government providers should tread more cautiously as consumers are more wary about sharing credentials across services
- User convenience needs to be part of the design, from enrolment through to everyday app usage. It is also imperative that the same experience applies regardless of the mobile device handset and operating system
- Consider how biometric authentication could increase user convenience, driving trust and adoption of new services. Biometric authentication is being embraced by consumers (as we learned in first part of this report). Alongside fingerprint readers, facial recognition and iris scanners are starting to roll-out as well. A good example of this can be seen in the announcement of **MasterCard Selfie Pay** or the iris scanning capability of some **Samsung phones**. Providers should continue to explore how they incorporate these features that are resonating with consumers. Providers can then use the subsequent user uptake as a positive proof point

The survey shows users want to rely on strong authentication for mBanking and demonstrated that if security is guaranteed, users are accepting of new solutions such as eGovernment services. As mentioned previously, these solutions have significant potential to streamline the way we access important tasks such as applying and managing identity documents, health, education, tax and even voting. Strong authentication allows industry players and governments to provide these **higher value services** for their **customers** or citizens.

In the next section, we will give an overview of the security solutions available which can be designed to meet end-users' expectations. Essentially, it comes down to the use of Software Development Kits (SDKs) which can be used to add additional and customizable security, in addition to what exists in the market such as built-in security features protecting the OS of handsets and commercial browsers, as well as anti-virus software.

Designing self-protecting apps

App providers need to implement end-to-end security architecture which can deal with new dynamic malware. Some solutions such as purpose-built software development kits (SDKs) can address the problem through security mechanisms that allow apps to:

- Defend themselves through coding techniques and cryptography
- Detect threats through secure environment detection
- React in the presence of threats: stop the execution, send an alert to a risk management server

Regardless of the strong authentication implementation, it must be reiterated that keeping a fluid user experience is paramount when considering authentication options.

Strong authentication

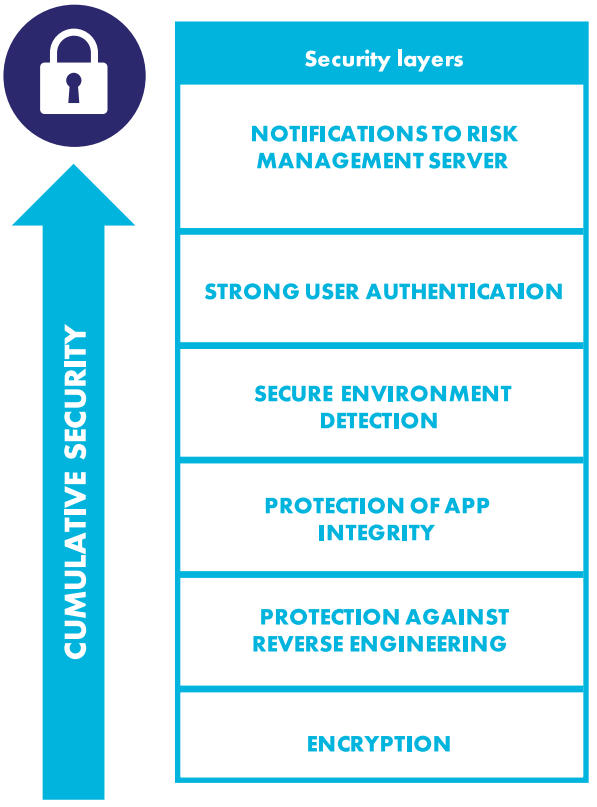
SDKs allow developers to design strong user authentication methods.

Biometric technology, which as we learned in part one of this report is particularly popular among end-users, is an innovation that's well suited to mobile. People trust that their fingerprints and faces are unique enough to act as their authentication key. Furthermore, if app providers want to explore other options for strong authentication, they could consider one-time passwords, or Out-of-Band (OOB) via Push, a method where a push notification is sent to the user's phone, requesting approval for any app login request. Secure PIN pads also warrant consideration as they are integrated in the app instead of using the default PIN pad of handsets, protecting sensitive authentication credentials such as PINs and passwords. In addition, SDKs also enable the design of digital signatures, which serve as another good example of a strong authentication method for securing critical transactions. However, regardless of the strong authentication implementation, it must be reiterated that keeping a fluid user experience is paramount when considering these authentication options.

The table below gives a summary of the different techniques of protection that SDKs can provide

EXAMPLES OF THREATS IN THE DEVICE	MOBILE SECURITY SOLUTIONS
Sensitive data disclosure such as passwords, user personal data disclosure (contact names, SMS, emails)	• **Encryption** and **strong authentication** for securing access to personal data
Unlocking of game licences, which can cause millions of $ of losses.	• **Code obfuscation** • This coding technique can help protect intellectual property and licensing
App programming code analysis: the logic of the codes can be revealed and exploited.	• **Code obfuscation** • **Anti-debugging** • **White box cryptography** • These techniques also help protect against reverse engineering
User interface: PIN/Password capture through key loggers (malwares) which can enable hackers to fraudulently log onto a user's online banking account, or fraudulently log on to remote enterprise resources and steal sensitive data.	• **Alternate virtual keyboard**, as part of the app design instead of using built-in keyboards • **Biometry** such as **fingerprint authentication** • Both solutions provide strong user authentication
Mobile device and passwords stolen and used by an unauthorized party, which could access user's online banking account or a user's online government accounts and steal enterprise resources.	• **Risk Management System** which can detect unusual user behavior and apply security policies accordingly • **Mobile Device Management (MDM)** featuring remote data wipe: in this case the user can remotely erase the phone memory and keep their personal data private
OS emulation replacing a genuine OS / phone memory cloning in order to fraudulently access online resources (bank, enterprise, government...)	• **Risk Management System** which can detect if the mobile device is not genuine and prevent unauthorized access to online resources, according to its security policies
The operating system of the device is corrupted, with lower access rights. This can happen when users change the security settings of their mobile devices, without realizing the potential risks. If they download malware, it can potentially control all the apps, since it will have "super user" rights	• **Jailbreak/root detection** for these coding techniques allows apps to detect an unusual or unsafe environment on the device and can stop it working or send an alert to the risk management server. • These techniques help protect an app's integrity
Transaction values modified: such as the amount of money that users want to transfer through mBanking for instance	• Anti-debugging • Anti-hook • Anti-tampering • These coding techniques help protect the integrity of transactions

Mobile software security, a layered approach



Depending on what is at stake, multiple security layers can be added, increasing the level of security

Layered security

To combat growing levels of sophistication from hackers, it is important to adopt a layered approach to security. It is not enough to rely on a single method of protection; there needs to be additional security layers dependent on what is at stake, whether that is first-time enrolment, or general use.

At the technical level, several layers of security can be combined in order to increase the overall level of security. Cyber-attackers are skilled at identifying points of weakness in the mobile ecosystem, so it is crucial to make it very difficult for them to attack each part of the app experience, using layers of security. SDKs enable this layered approach, hence why the use of them is a key recommendation of ours when it comes to protecting against cyber-attackers.

Risk Management

As you can see from the illustration of layered security, risk management is a key part of this approach. Cyber threats are not static, but constantly evolving and increasingly unpredictable, meaning security systems can fast become obsolete. The dynamic nature of the threat requires a flexible risk management system, which can respond to new situations and implement adaptive security policies whilst the apps are used on the field. These systems can detect unusual user transaction patterns, evaluate the risks of a transaction and remotely stop the transaction or ask the users for further authentication, to minimize the risk. Crucially, this analysis is executed in real-time so as to counteract threats immediately, before it's too late.

> To combat growing levels of sophistication from hackers, it is important to adopt a layered approach to security.

> Cyber threats are not static, but constantly evolving and increasingly unpredictable.

Conclusion

A secure mobile ecosystem is a wide topic, encompassing the backend, network and device. However, in this report we focus on mobile app security; apps are being used increasingly by key players in the industry and governments – as this happens, more and more threats in this space continue to arise.

At every step of the user journey, protection is crucial. Strong authentication and identity protection are necessary to ensure mobile software receives adequate protection.

Moreover, it is crucial to include user convenience and the 'psychology of security' as part of the security design, in order to trigger service adoption. In particular, the use of biometry such as fingerprint readers, facial or iris recognition is becoming more popular.

It's also worth noting how the research has demonstrated there is widespread awareness of cybersecurity issues. Consumers clearly value robust protection to the point that many would pay a premium for guaranteed security.

In a world where cyber threats are constantly evolving and consumers have access to an unprecedented number of valuable services through their smartphones, it is important each player is prepared. Cybersecurity cannot be treated as an afterthought; effective risk management and evaluation systems need to be in place to protect end-users, otherwise trust in mobile apps will be severely undermined and the full potential of mobile will not be achieved. We know the opportunity is out there; we know users would embrace digital identity for example if they knew their mobiles were 100% secure (see page 15). **Electronic Identification and Signature (eIDAS) Regulation** is already law within the EU today; it's now just a question of gaining momentum.

As our lives increasingly exist on mobile, it is imperative we can trust the devices and services we use every day. This is why Thales' mobile security solutions are purpose-built to support multiple security frameworks, both at the software and hardware level, to deliver best-in-class digital security and facilitate service deployment in a fragmented mobile market.

Thales works across numerous industries, with banks, governments, mobile network operators, OEMs, transport operators, and automotive manufacturers... By working together, we can develop a secure ecosystem that mitigates the ever evolving cyber security threat landscape.

THALES

> Thalesgroup.com <