fime

eBook

Biometric authentication. Making innovation possible.

Tips and considerations for successfully developing, integrating and launching biometrics.

May 2021

fime.com

Contents

Biometrics is the answer to a smooth user experience without compromising on security. With the huge success in mobile, consumers are familiar with the technology and its benefits. Biometric vendors and device OEMs have an opportunity to innovate and differentiate.

Jean Fang at Fime
Authentication Product Manager

Successful projects require careful strategic planning and execution to turn complex regulatory, security, performance and user experience challenges into opportunities. Failed products or uncontrolled bias damage brands, high-quality products grab market share.

Joël Di Manno at Fime
Authentication and biometrics laboratory
Service Line Manager

1. Market momentum.

Biometrics are a rare example of technology which enhances both convenience and security.

From face to iris, voice to behavior, these technologies are already adding value to sectors like financial services, telecoms and even government administrations. **Now, a range of influences have pushed biometrics right to the top of the agenda.**

Touchless, hygienic authentication and identification solutions have become critically important amid the pandemic.

And the shift to remote working has required secure and flexible physical and logical access management. At the same time, consumers familiar with biometrics from their smartphones are keen to do away with the PINs and passwords that dominate other areas of their lives. This trend only looks set to grow.

Key emerging use-cases include:

- **Payment authentication** including biometric payment cards and meeting Strong Customer Authentication requirements.
- **Physical and logical access control** like IoT, automotive, transport or electronic devices in the home and at work.
- **Government administrative projects** such as ePassports and driving licenses.

These use-cases and others are driving massive growth across the biometrics market.

Already valued at some 20 billion USD in 2020, one estimate predicts a 35% CAGR across the next 5 years.

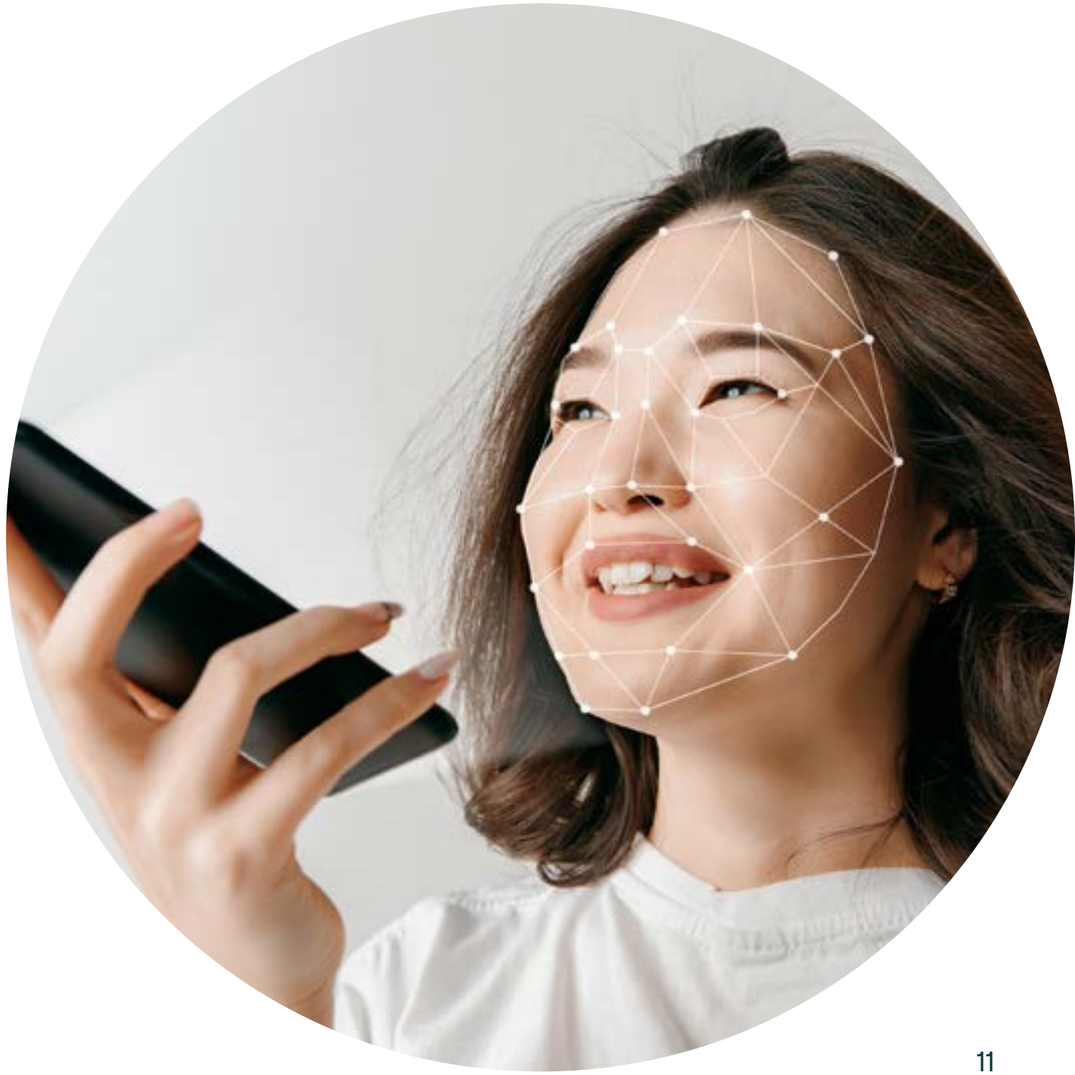
The opportunities for vendors and device OEMs are significant.

Considerations for success.

To succeed in this competitive market, vendors and OEMs must consider:

1. The interplay between performance and security.
2. Ensuring a frictionless user experience (UX).
3. Shifting industry and regulatory requirements.
4. How poor product performance could impact brands.

Achieving this is complicated by the challenges of working with an innovative, evolving technology and within a fragmented and largely non-standardized ecosystem.



This eBook explores some of the key considerations vendors and OEMs face when developing and integrating biometric solutions.

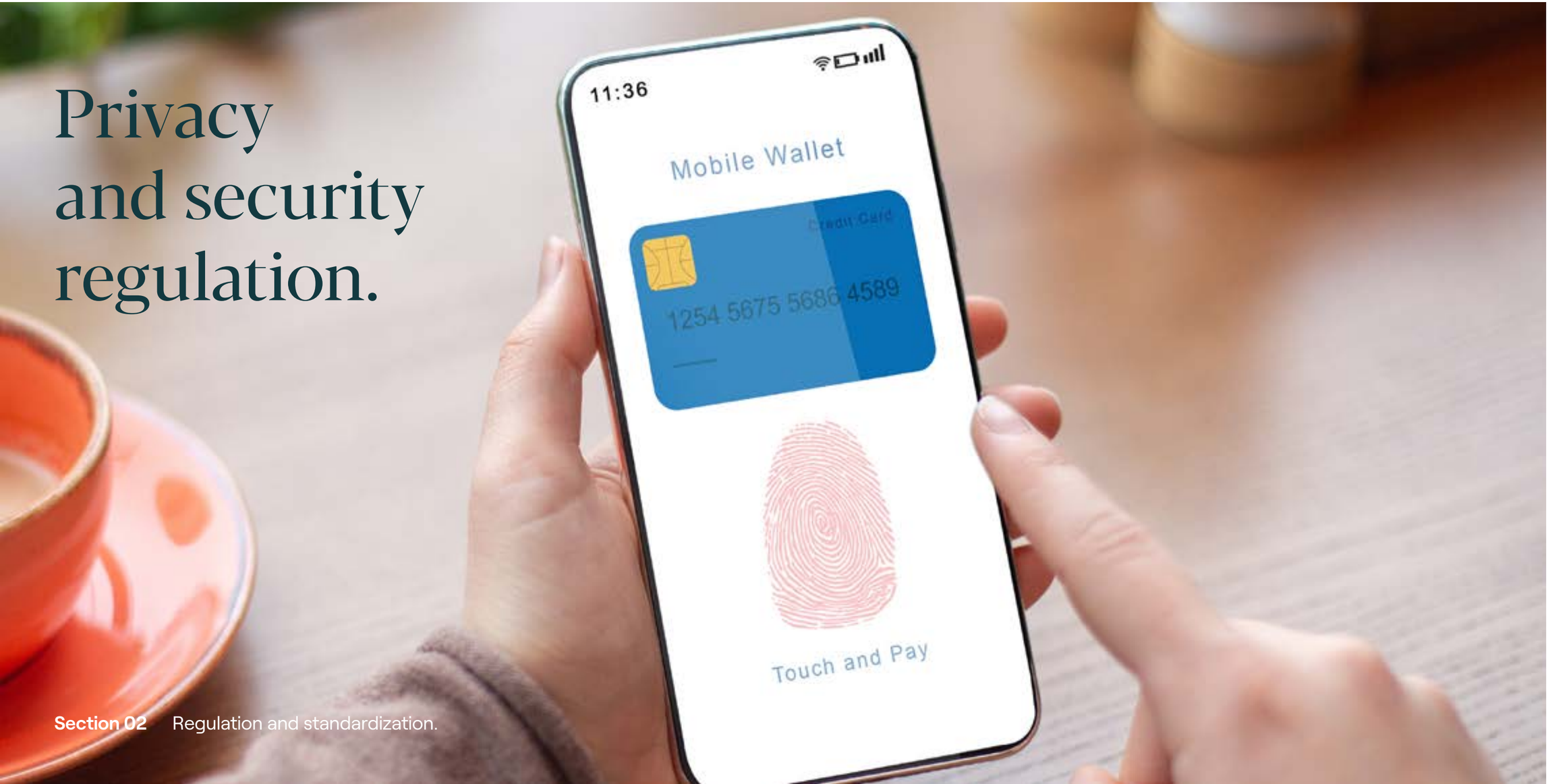
It outlines the need for strategies to be clearly defined, and highlights the role testing can play in biometric success.

2. Regulation and standardization.

While biometric technology has been deployed at scale, there are surprisingly few regulations and standards specific to the technology.

There are **two main sources of regulations or standards** which apply to biometric projects:

Privacy and security regulation.

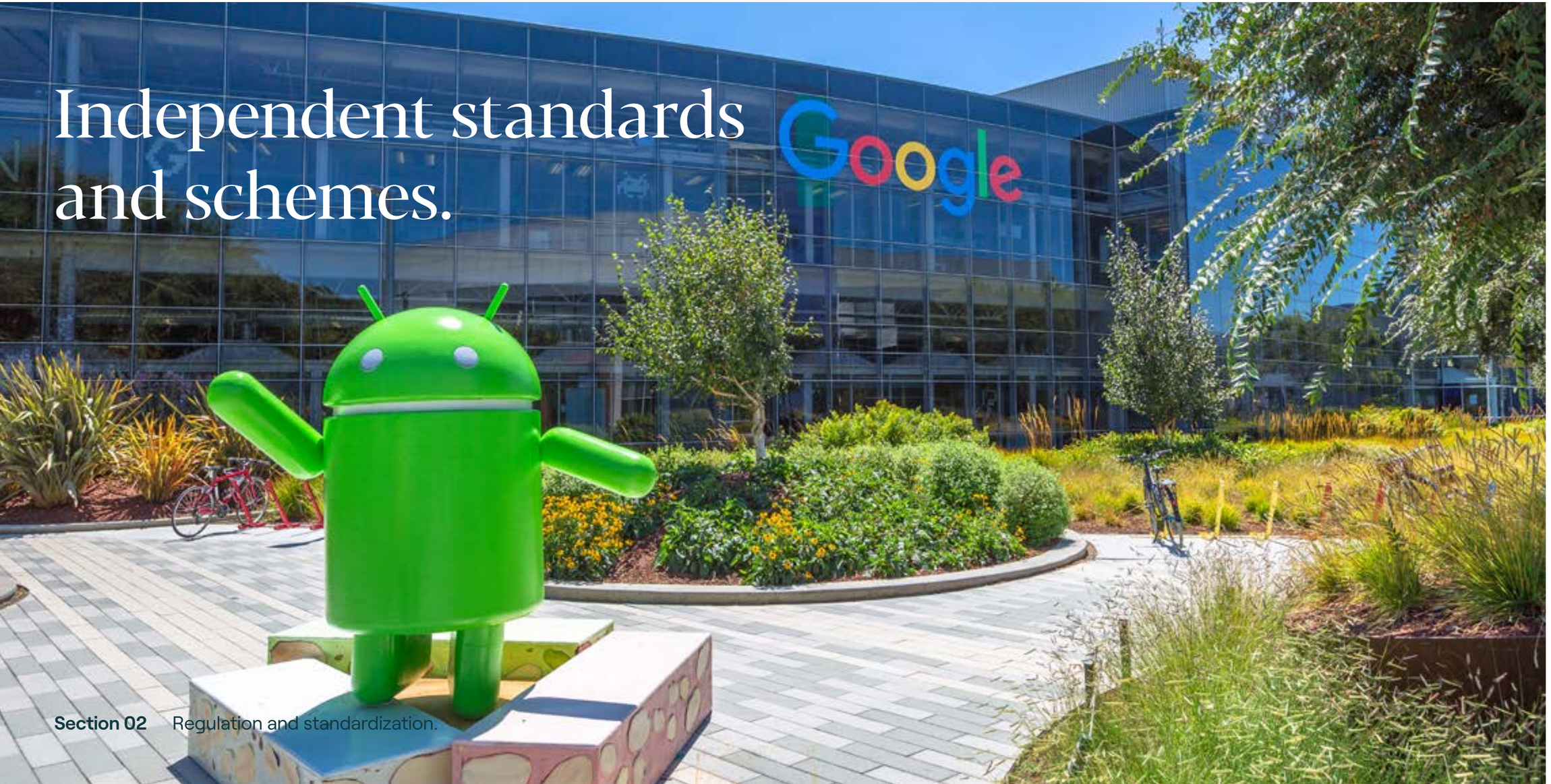


Almost all biometric projects will fall under general privacy and security laws, as processors of personal biometric data. Notable examples include:

- The General Data Protection Regulation **(GDPR)**, which applies to over 500 million European Union citizens.
- Japan's Act on Protection of Personal Information **(APPI)**.
- The Californian Consumer Privacy Act **(CCPA)**.

Such legislation has strengthened in recent years and places strong obligations on developers.

Independent standards and schemes.



A number of independent standards and schemes which specifically reference biometric solutions are beginning to make important progress in filling the regulatory gap.

These originate from industry organizations such as the FIDO Alliance, various ISO Working Groups and NIST, as well as from individual companies, most notably Android (Google), Mastercard, Microsoft (Windows Hello), and Visa. They are often voluntary, and even when mandated – such as Mastercard's Biometric System on Card (BSOC) standard – they are organization – specific, rather than regionally or internationally standardized.

The challenges of fragmentation.

Despite the value of these schemes, it is clear that a large degree of fragmentation persists. In the context of a technology that is still evolving and diversifying, navigating different standards creates additional complexity for developers and manufacturers.

These fall into three main challenges.

1. Interoperability

As deployments expand and diversify, inconsistent standardization can result in poor interoperability, a lack of adaptability and a weaker user experience.

2. Certification

Individual company and organization standards are increasingly requiring certification. Given the lack of standardization among different schemes, developing a product which satisfies multiple standards requires deep expertise and sophisticated testing strategies.

3. Benchmarking

'Benchmarking' – the practice of comparing performance metrics to industry best practices – can be a particular challenge in the absence of robust regional or international standards. Simply put: companies can struggle to assess how effective their product's performance is.

3. Security and user experience.

Ensuring strong security and privacy is key when developing and deploying any new technology.

It is essential to build confidence and trust, especially for technologies which processes our personal data.

To mitigate security threats, vendors and OEMs need to identify, evaluate and address potential weaknesses.

For example, a solution's ability to resist spoofing – faking biometric identifiers to enable false authentication – can be evaluated through Presentation Attack Detection (PAD) testing. This simulates anti-spoofing capability against a variety of spoofing instruments and scenarios in a controlled environment, providing crucial insight into security performance.

Security vs UX.

At the same time, the appeal of biometric authentication is that it combines convenience with security. **Overly-stringent security can negatively impact the UX, requiring implementations to find the right balance.**

This is best understood through a comparison of the False Acceptance Rate (FAR) and False Rejection Rate (FRR).

- **A low FAR** – i.e. a low number of successful authentications without the use of the correct biometric identifier – is a key indicator of a solution's security.

- **A very high level of security raises the FRR** where the correct biometric identifier has been presented, but authentication fails. This creates friction, potentially preventing access to a personal device, or declining a biometric payment.

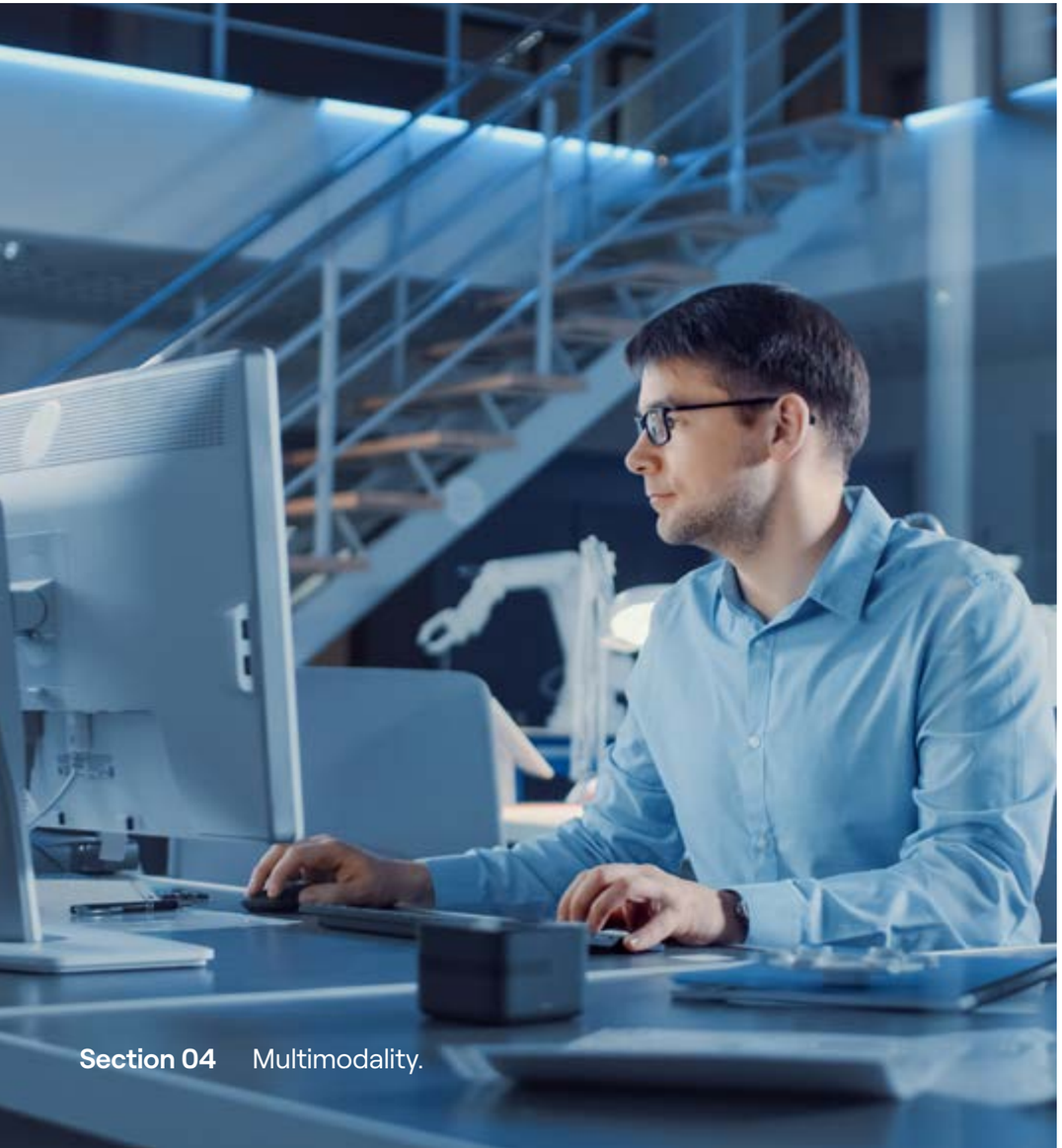
Achieving an optimal FAR / FRR balance is therefore a key consideration in product development.

Rigorous testing to evaluate the exact trade-off is once again a key tool in ensuring this, as is strong benchmarking and initial strategy.

4. Multimodality.

After a decade of smartphone integrations on a mass scale, fingerprints are the most familiar biometric modality. Still, there are a number of biometric modalities which each have distinct benefits and features:

- **Facial**
- **Iris**
- **Voice**
- **Palm**
- **Behavioral**



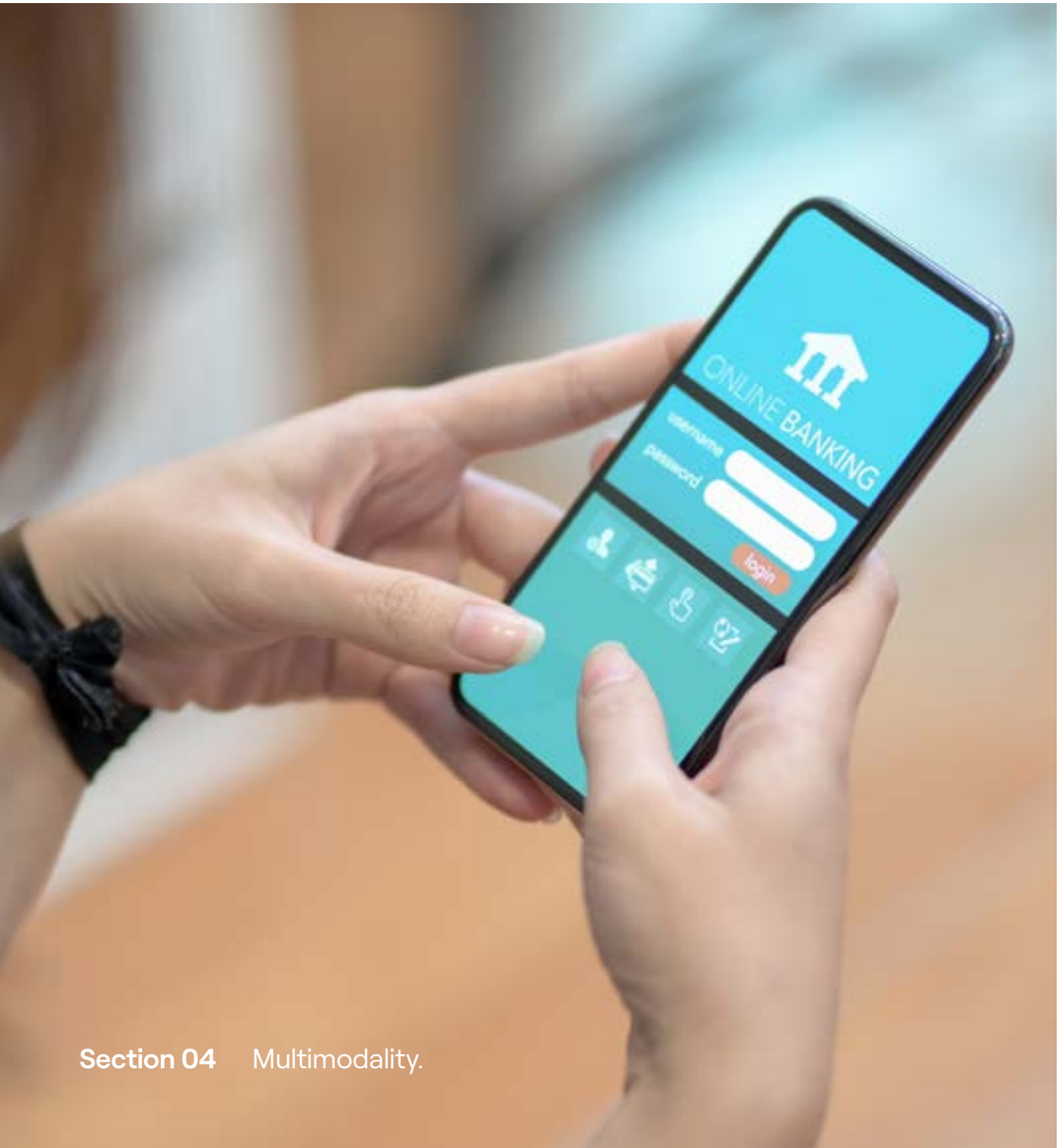
Technology vendors need to constantly evaluate new and existing solutions to optimize them for the real world and OEMs need a clear strategy and process to define which biometric modality is best suited to their devices. To do this, they should take into account factors like cost, UX, speed and security.

Multimodality implementations – where solutions combine multiple biometric identifiers – are also becoming more commonplace. **Depending on deployment requirements, multimodal solutions can serve a variety of aims.**

Security.

If it is difficult to spoof a fingerprint, it is almost impossible to spoof a fingerprint and an iris scan.

Requiring input of two biometric identifiers, for example, doubles the challenge for spoofers – thus boosting security.



Convenience.

Authenticating two factors might be appropriate in some circumstances, but too much in others. **Behavioral enables multimodality authentication without increasing the burden on the user.**

Behavioral data can be collected in the background, allowing the user to authenticate with their voice, for example, when they want to complete an action.

Adaptability.

Environmental factors can make some biometrics challenging.

Fingerprint authentication is not helpful when wearing gloves on a cold day, and facial biometrics can be blocked by face masks.

A solution equipped with multiple modalities enables users to switch between the most appropriate modality.

The technology’s multimodal potential is both an opportunity for innovation and a source of additional complexity for developers.

Determining which modalities will serve deployments best and balancing their performance is challenging.

Vendors and device makers do not have to navigate the regulatory, security, performance and implementation challenges alone.

5. Four steps to biometric success.

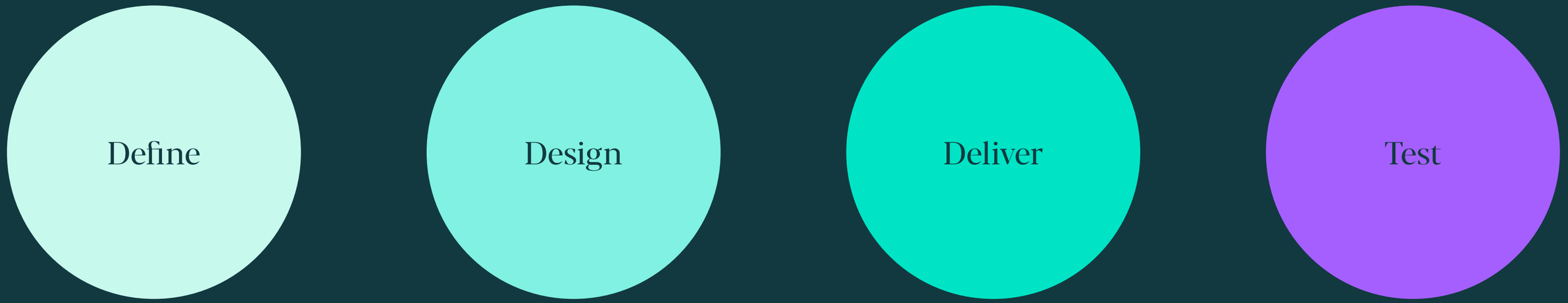
With the right approach, biometric product vendors and device OEMs can save time and money. They can also maximize innovation and compliance by ensuring their strategy is well defined from the start of projects.

To do this, it's important to:

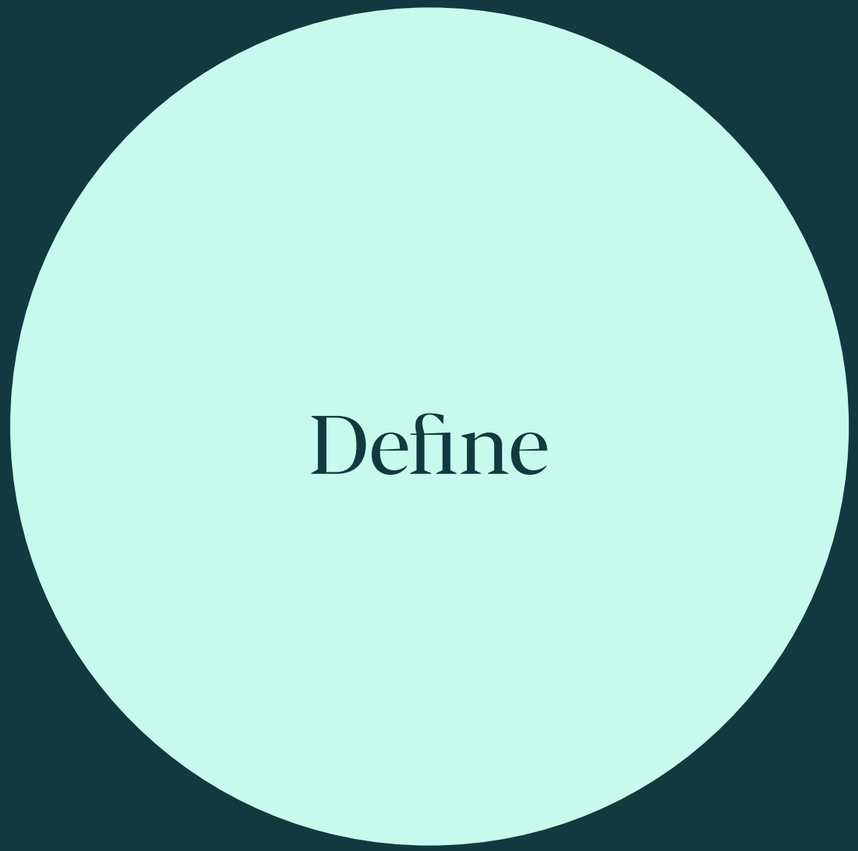
1) Evaluate ecosystem trends and standards.
2) Determine the right strategy.
3) Test for security and performance.
4) Outline a certification plan and launch.

Throughout the process, Fime supports stakeholders in four different stages.

Checklist to ensure a smooth integration project.



Define Design Deliver Test



Stage one – Define to get ahead.

Understand and answer critical business questions to formulate your technical strategy.

- Define project and business requirements, including:
  1) Analyze the market & opportunities.
  2) Benchmark competition & technologies.
  3) Conduct cost analysis & financial modelling.
  4) Study customer needs & user experiences.

- Conduct impact and risk analysis, to understand regulatory and operational implications at technical and corporate levels.

Define Design Deliver Test

Design

Stage two – Design to improve efficiency.

Choose the best technical and cost-effective options, and design an efficient test strategy.

- Design solutions with a focus on interoperability, security, and performance.
- Develop the right test strategy, plans, methodology, tools and quality assurance plan.

Define Design **Deliver** Test

Stage three – Deliver to make it happen.

Roll out your chosen solutions and develop ad-hoc test plans and tools.

- Full project management and development of specific test solutions, including test tools, libraries and test studios for your specific needs.

- Undertake knowledge transfer to enable successful integration and management of biometric implementations.

Define Design Deliver Test

Stage four – Test to ensure trust.

Test solutions for compliance and quality assurance.

- Testing products and devices, including physical, interoperability, aging, sensor quality, performance, spoof resistance, functional, environmental bias and live user experience.

- Harnessing the latest artificial intelligence and machine learning techniques to validate products against the broadest set of use cases, requirements and benchmarks.

6. Optimizing solutions and integrations.

We believe that biometrics have a huge role to play in almost every industry you can name.

Our homes, workplaces, transportation and more will soon be simpler and safer. But we are at a crossroads. Huge success in mobile does not simply equate to every other device.

With a complex landscape of rapidly changing regulations and requirements, technologists and device makers need assurances that their products and solutions will perform well and be secure in the real world.
This is key to protect and empower users, and prevent damage to brands.

Real world use cases are not the same as certification conditions. Deep expertise in product design, delivery and testing is needed for stakeholders to have confidence in the performance and presentation attack capabilities of their technologies. Working with expert partners means you don’t need to invest time and money in expanding and upskilling internal teams, **getting innovations to market faster.**

Share your challenge.

Our Fime experts are here to help you make innovation possible, from defining, designing to delivering and testing your products and services.

Visit fime.com
or contact sales@fime.com