Self-service enrolment kiosks

Second generation

Delivering new standards of security for governments and their citizens

THALES
Building a future we can all trust

Executive summary

Nearly two decades after the world's first self-service enrolment kiosks were introduced, a second generation is now being deployed. As a result, governments worldwide are embracing new opportunities to enhance the security, convenience and efficiency of their registration processes for biometric-based credentials such as ePassports and eID cards.

Since the beginning of the 21st century, issuance of official documents based on the holder's unique face, fingerprint and iris data has grown exponentially. But so has the threat posed by ID fraud and cybercrime. In response, new standards and regulations have been implemented for biometric security and data privacy. Over the same period, attention has shifted beyond the integrity of the document itself to include the need to strengthen registration processes against techniques such as spoofing and face morphing.

For a growing number of countries, self-service kiosks have been central to these efforts. By combining the inherent advantages of live enrolment with a range of sophisticated anti-fraud techniques and technologies, the latest generation of self-service kiosks provide another powerful asset in the on-going fight against identity theft, fraud and hacking.

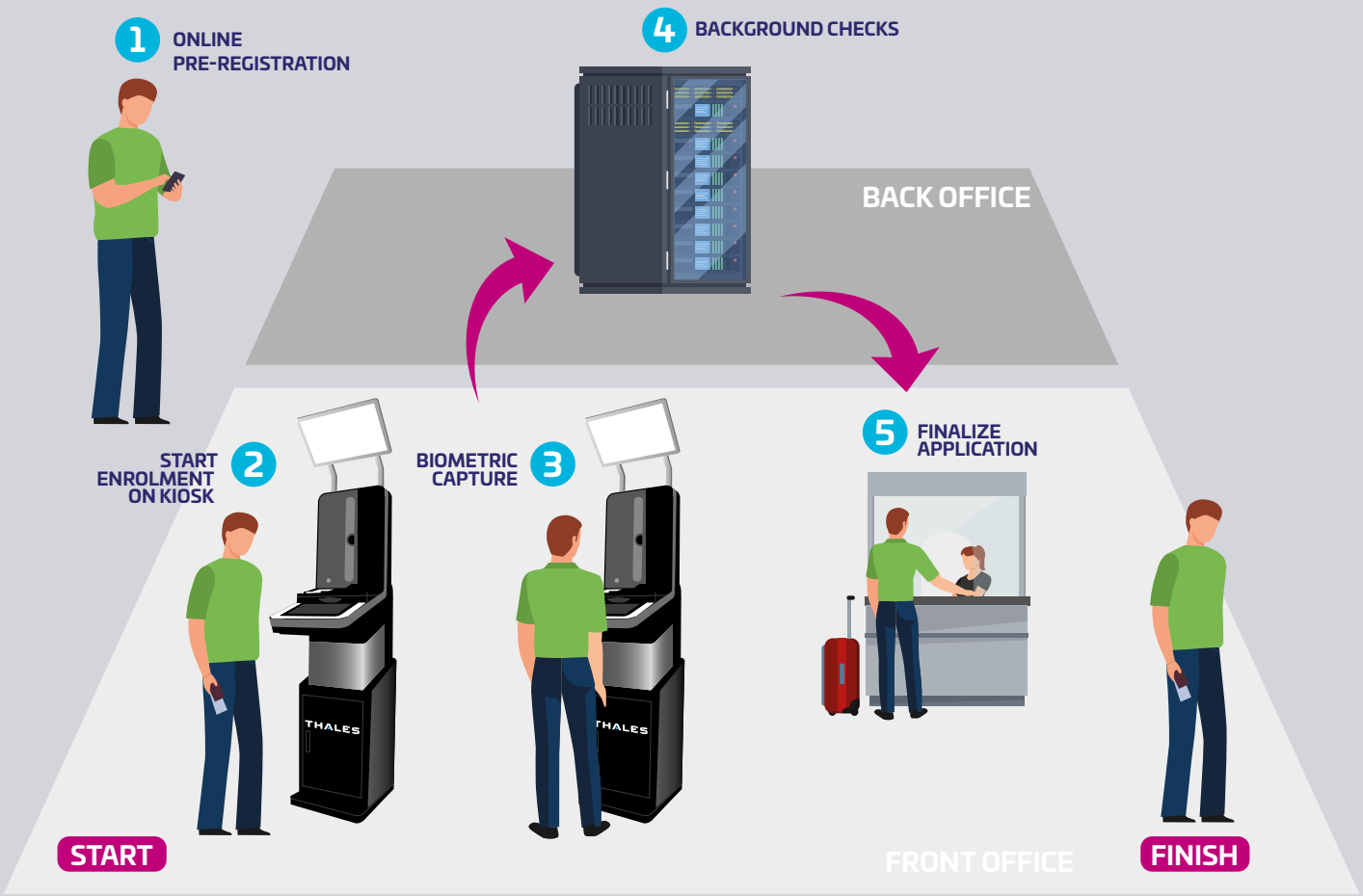
However, security is far from the only consideration driving the reinvention of registration processes. Governments are equally keen to enhance their customer service standards and reduce operating costs. Here again, the second generation of self-service enrolment kiosks can have a transformative effect. What's more, they are aligned perfectly with one of the more notable trends redefining modern life. From accessing public transport to negotiating passport control, people are increasingly comfortable with the idea of using self-service solutions for a faster and more convenient experience.

Addressing the limitations of conventional registration processes

Traditionally, the enrolment process for passports and other official documents has been slow, inconvenient and bureaucratic. For many citizens it involves posting physical forms and photographs to the issuing body. If any of these submissions are subsequently rejected (for example, if the photo does not comply with requirements) the likely result is further delay and frustration. Furthermore, citizens are often obliged to arrange face-to-face appointments with government officials. Again this can involve long waits and yet more inconvenience.

In contrast, self-service enrolment is simple and straightforward, and puts the citizen in control.

What does kiosk-based enrolment look like?



Following any pre-registration procedures, citizens can quickly and easily complete the necessary steps at their own pace, at an intuitive and inclusive self-service kiosk. By removing the need to post items or make face-to-face appointments with officials, the entire journey becomes fast and frictionless.

What's driving adoption?

Right around the world, three stand-out factors are fuelling government investment in second generation kiosks:

Citizen convenience: governments are prioritising the need to simplify and speed document application processes

Self-service enrolment kiosks represent a powerful and highly visible means of improving the service offered to citizens. By enabling a one-stop-shop approach, queuing and delays when applying for and updating passports and other official credentials are reduced dramatically. Moreover, the frustration caused by rejected postal applications is eliminated. Instead, the acceptability of documents and biometrics is assessed in real-time. Any issues and problems can be dealt with immediately.

System security: governments are demanding increased protection for personal data and official documents

Document issuing bodies need to ensure that photos submitted as part of the registration process are a true representation of the applicant. The integrity and quality of fingerprints and signatures must also be assured. In response, the latest generation of kiosks offer best-in-class biometric recognition technology and full compliance with the latest standards. As a result, they are highly resilient against even the most sophisticated attacks, including fake finger, spoofing and face morphing.

Inviting citizens to perform live enrolment within a controlled environment offers obvious security benefits. Furthermore, kiosks can integrate systems that detect any attempt at deception by using a friend or associate to submit biometric data on behalf of someone else. Kiosks also provide governments with a proven means of complying with data protection regulations, and the highest standards of protection for citizens' personal information.

System reliability: governments are seeking to optimise value for money and return on investment

Enrolling citizens for ePassports, eID cards and other official documents is a critical, public-facing process. Any problems are likely to have a serious impact on the reputation of the department concerned, and levels of satisfaction among citizens.

Around the world, governments are therefore emphasising the need for systems to operate reliably and intensively over a multi-year lifespan. Kiosks also pave the way for significant reductions in overall operating costs, and the redeployment of staff to roles that optimise their productivity and effectiveness.

The evolution of self-service enrolment

Governments worldwide are actively considering deployment of second generation self-service enrolment kiosks. A number have already done so. However, the concept itself is nothing new. As far back as the mid-noughties, Sweden, Portugal and Malaysia were at the forefront of this self-service revolution. Other countries have since followed suit, and adoption in now on a steep upward trajectory.

The rise of the ePassport – and more sophisticated fraud and cyber-threats

Roll-out of self-service enrolment kiosks has gone hand-in-hand with the evolution of ePassports. Here again, Malaysia emerges as a trailblazer, introducing the world's first ePassport in 1998. By the following decade, a few dozen more countries were also issuing passports featuring an electronic chip for storing the holder's biometric data. In 2004, the EU (European Union) set a goal for all member states to introduce facial images in electronic chips in passports by 2009.

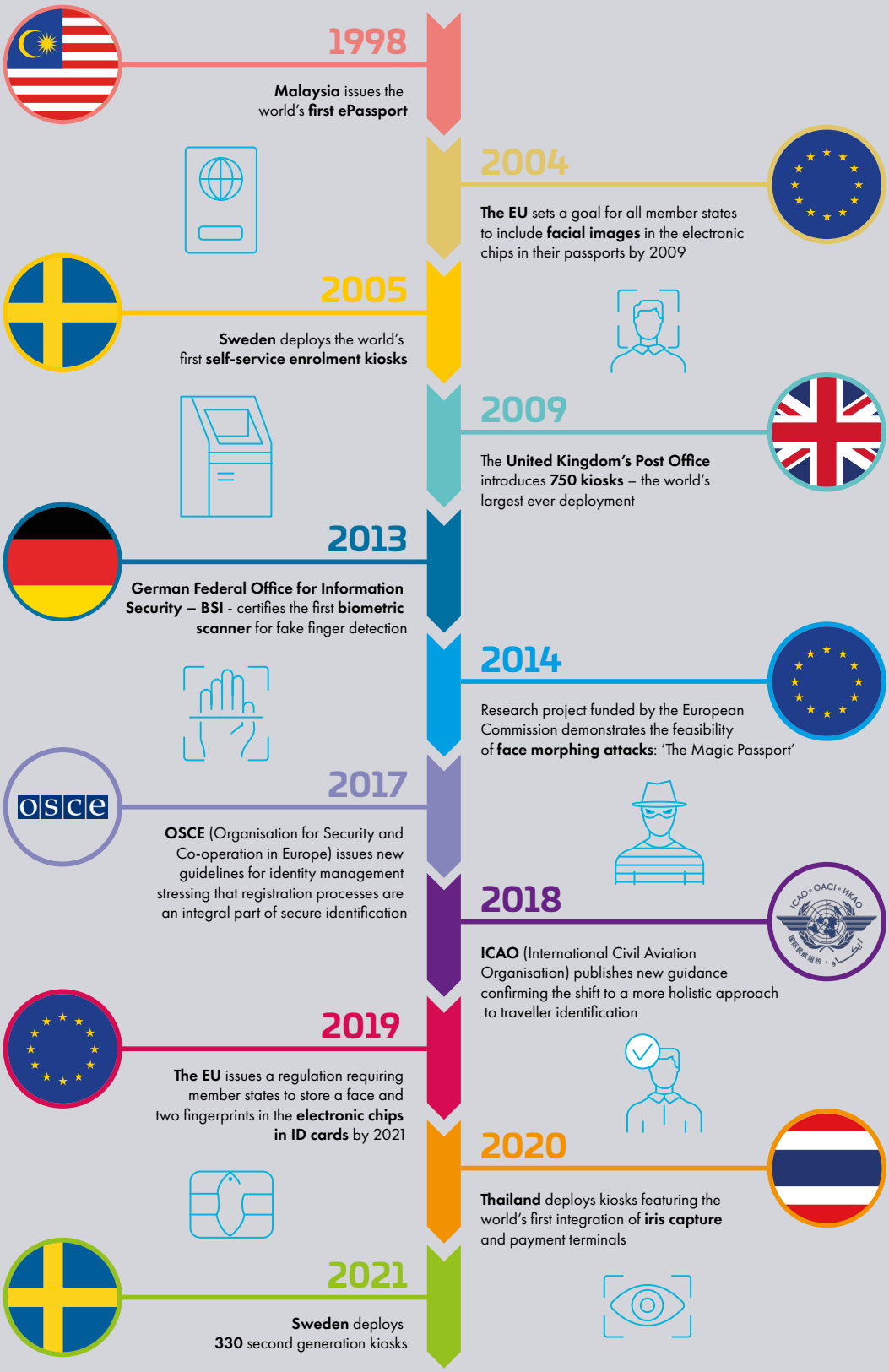
The issuance of official credentials based on biometric data was driven primarily by a desire to address identity fraud. However, within a few years there was growing concern about potential vulnerabilities in ePassports, and biometric identification in general.

Three of the most significant threats were identified as:

- **'Fake fingers' –** designed to fool biometric fingerprint scanners
- **'Spoofing' –** where a still image is used to fool a live facial recognition system
- **'Face morphing' –** where two different facial images are merged digitally to create a picture that resembles both these people closely enough to avoid easy detection by the naked eye.

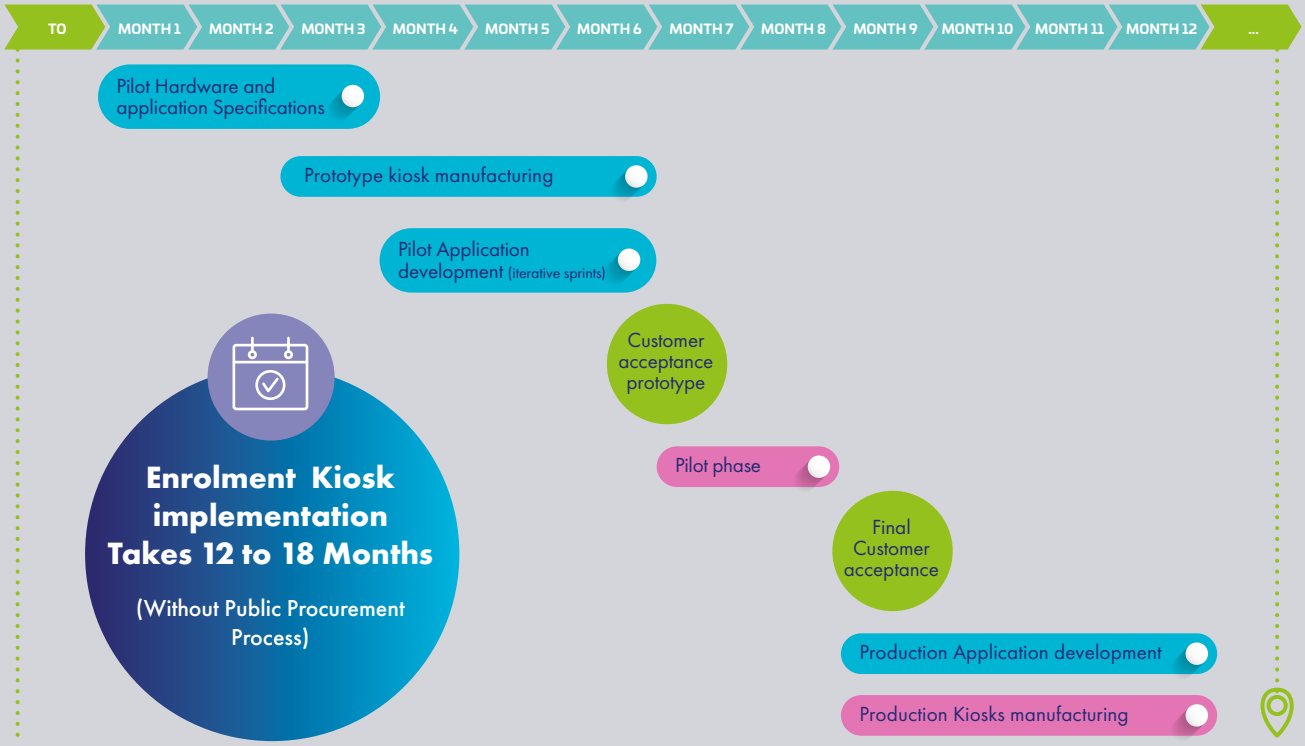
These threats have implications for the integrity of the documents themselves and associated enrolment processes. Over the past two decades, governments and various international bodies have therefore taken the lead in introducing new standards of protection against ID theft and fraud.

Key dates and landmarks



Managing the deployment of self-service enrolment kiosks

Deployment of new enrolment kiosks typically takes between 12 and 18 months. Each project is unique, but common factors likely to have a significant impact include the level of customisation specified by the customer, and the extent of any changes required after the initial pilot.



Making the most of the pilot phase

The pilot phase is particularly significant. Although some countries are now migrating from first generation kiosks, for most governments the pilot will represent their first experience of this innovative approach. Every customer, location, country and culture is unique; it is impossible to predict precisely how end users will react to the introduction of kiosks.

Given that kiosks invariably represent one brick within a wider system, the pilot will also play a key role in highlighting exactly how the new technology interacts with existing processes. Similarly, it will gauge the suitability of the environment in which the kiosks are expected to operate. The human factor is important too. Different customers employ different levels of staff supervision for their kiosks, so this is another important area for investigation during the pilot phase.

Above all else, it is vital for customer and supplier to identify any changes needed ahead of full scale deployment. Implementing modifications immediately after the pilot phase is invariably more economic than doing so at a later stage.

The Thales Solution

Thales brings over 30 years' experience in biometrics to the development, deployment and support of self-service enrolment kiosks. Building on the company's work in fields such as policing and law enforcement, Thales is now a leader in self-service citizen enrolment. To date, the company has installed over 1650 kiosks for customers worldwide, more than any other supplier in the market. Over 20 million people have now enrolled with a Thales solution.

Thales' self-service solutions comprise the three key building blocks of any successful system: hardware, software and support:

- Thales' self-service solutions comprise the three key building blocks of any successful system: hardware, software and support:
- The core Thales design is characterised by accessibility and inclusivity. Built in accordance with the Americans with Disabilities Act (ADA), the standard unit is suitable for people who use wheelchairs. Crucially, the Thales kiosk adapts to the user, not vice versa. Motorisation of both the console and the camera enables a best-in-class height range of 90cm to 210cm.
- Safety is a priority. High levels of kiosk stability are combined with an absence of sharp edges, or gaps that might pose a risk of finger pinching and trapping.
- The modular design of the unit minimises the need for complex and costly customisation; additional hardware such as payment terminals can be integrated easily. This also ensures that citizens can perform all the necessary processes in one place.
- Thales' extensive, in-house expertise in biometric scanning and software is evident throughout. Key features and options include fingerprint scanners with integrated fake finger detection, certified to ISO 30107-3, and facial recognition with sophisticated liveness detection. Enhanced biometric capture and image quality is based on Thales' own algorithms. As a result, photos and scans are far more likely to meet requirements at the first time of asking. If required to match a document to the holder, 1:1 facial matching can also be integrated.
- A supervision camera protects against person-swapping during enrolment
- Security-by-design approach ensures the highest standards of encryption and protection of personal data
- The UX (User Experience) is best-of-breed, designed to reflect the digital interfaces that people now use routinely in their daily lives. Voice prompts and 'landing lights' further contribute to an intuitive and accessible experience, maximising citizen adoption and speeding enrolment.
- To provide optimum support for customers, from initial design right through to deployment and field maintenance, Thales has certified teams of IPMA and PRINCE2 qualified professionals based around the world. Full compliance with ISO 37001 ensures that transparency and accountability are embedded throughout the project workflow.

Note

THALES

Building a future we can all trust

Tour Carpe Diem - 31 place des Corolles
92098 Paris La Défense - France
+33 (0) 1 57 77 80 00

thalesgroup.com