



[thalesgroup.com](https://www.thalesgroup.com)

THALES
Building a future we can all trust

Trusted **digital identity** for
everyone
everything
everyday



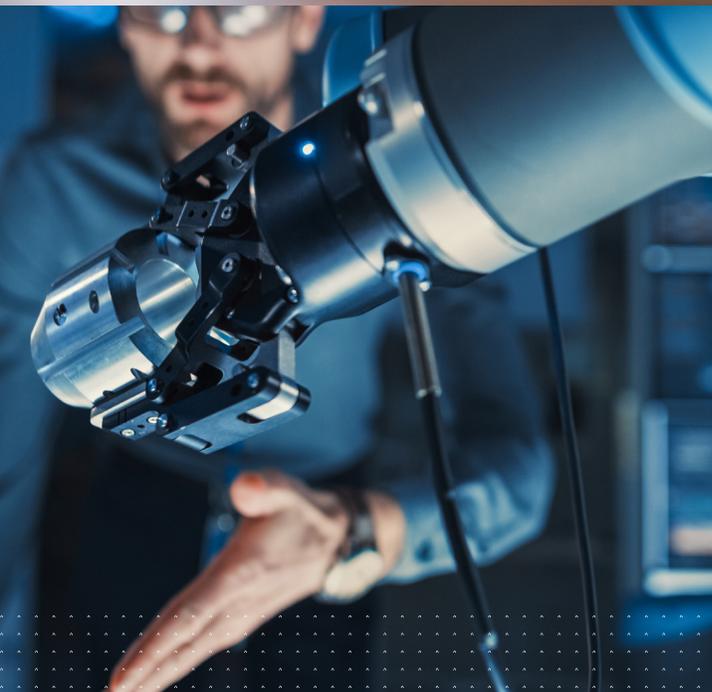


At Thales, we have a vision of a more secure future.
A future we can all trust.

As technology transforms our lives, secure proof of identity,
and authentication for connected services become ever
more important.

We are world leaders in delivering secure digital identities,
and the means to verify them, for everyone and everything.
Already trusted by governments and enterprises globally,
our certified solutions deliver the robust yet smooth
interactions that keep your world moving, your business
growing and digital identity secure, every single day.
Building a future we can all trust.

Digital Identity by Thales



What is Digital Identity?

Keeping billions of daily digital interactions secure

Trusted Digital Identity from Thales is about more than an individual technology or process. It is about enabling people, businesses and governments to have confidence in the digital interactions that take place every minute of every day.

Everyone knows how to prove who they are in a physical context. We are used to official ID documents and in-person identity checks. Digital identities are needed to ensure people can trust online service providers and vice versa.

These can take two forms, the first is a digital version of an official physical identity document, such as a digital driver's license. The second is a credential for accessing online services. This is created through an initial identity verification process usually involving a check against an official ID document and some form of biometrics.

Already, many governments and businesses rely on Thales to verify the identities of people and things, onboard them for new services, grant access and encrypt the data that they run on.

Why it's important

Tackling threats and opening up opportunities

Every organisation around the world is in the midst of a digital transformation. Whether you are a local or national government or a global enterprise, the demand for trusted digital interactions is rising.

Trusted digital identities are essential for digital transformation. As business growth depends on these digital services, organisations need trusted identities to support rapid development and reduce fraud. Adoption of the cloud, remote network connections and home working, as well as the COVID-19 pandemic, has accelerated the demand. Traditional options such as passwords are often not secure enough. Others are inconvenient. So trusted digital identity is required to create frictionless experiences while supporting businesses and organisations to achieve compliance.

This new era also brings opportunities. Trust is an important currency in the digital world and if you can offer robust digital identity then consumers and citizens will be able to depend on you. Whether it is accessing online services or securely connecting devices, successful organisations will be those that are trusted and make it easy to identify people or objects while maintaining operational efficiency. The imperative is to create digital identity that matches the needs of your sector, of your regulator and your users so you can create and maintain this trust.



Trusted **digital identity** for
everyone
everything
everyday

Why Thales?

Over the years we have built the capabilities to cover the entire identity lifecycle. From physical access and documentation to technology infrastructure and applications, we offer a chain of trust for organizations and convenience for end users.

It starts with expertise. Our services have been trusted by governments, businesses and individuals for generations. As the world becomes more and more digital, it is still our people that make the difference.

They not only provide the knowledge and technical expertise at the start of a project but they see it through and are on-hand to support our customers whenever they need us. They understand the nuances of different sectors and organisations. Importantly, they understand what motivates people and put the user first to ensure any new digital identity project delivers success and rapid adoption.

Thales is well established as a leader in providing digital and physical documents to governments. Our footprint also covers 30,000 organizations in 180 countries. We may be a global operation but we have people 'on the ground' who bring local know-how, experience and cultural understanding too.

Digital identity is part of our DNA. We are already at the heart of multiple markets – from telecoms and government to financial services – and share best practices between our teams. We know that our pivotal position in the digital identity ecosystem and collaborative approach with partners means we can find or develop a solution for our customers. There are many more people who work hard behind-the-scenes at Thales to ensure every service we provide is seamless for our customers. Testing infrastructure security. Ensuring compliance with the latest regulations. Advancing biometric technology.

In fact, innovation is critical across Thales. Without exploring new ideas we could not offer the kind of future-proofing our customers need. We also know how innovation empowers people. As markets from financial services to mobile communications switch directions, we must still be able to support them. So we continually develop robust, scalable digital identity services to match those changes – from securing mobile payments to protecting emerging 5G networks. As a Group we invest heavily in R&D, and our approach to innovation has even won awards, including not just one but two Nobel Prizes for Physics.

180

national identity programmes supported by our technology

700

million mobile subscribers rely on our SIMs and services

Trusted Digital Identity

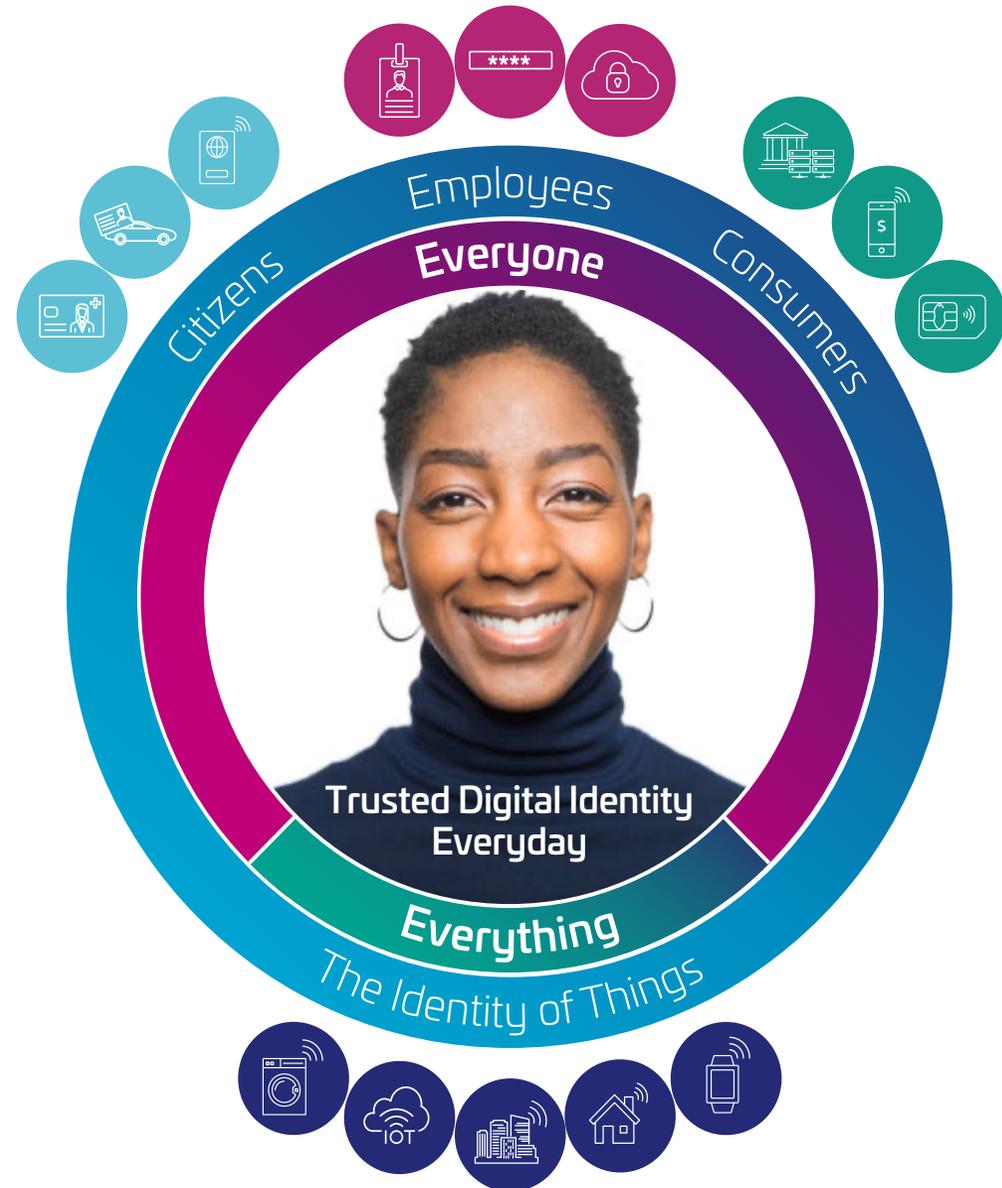
for **everyone** and **everything**

We have always been a leader in physical identity. And we have applied this expertise to our digital identity services. For citizens, consumers and employees around the world, we enable access to an rapidly growing number of online services. Many digital interactions happen on a person's smartphone, of which there will be 4.3bn in use by 2023*. Our 30-year presence in the telecommunications sector makes us best placed to support remote and mobile access to the things people need in their everyday lives. Whether that is tax records, bank payments or corporate systems, we help everyone go about their digital lives safely and securely.

We are specialists in digital identities and data protection for the rapidly expanding Internet of Things (IoT). Demand for IoT devices means that billions of new connections are made every year. From smart home devices to remote utility meters, these objects produce billions more data points that must be secured. For the IoT to be trusted, it requires a sophisticated identification process to ensure that the device, application software, and data can be trusted. We understand that these new corporate assets are the focal point of a new and exciting business. That is why our trusted digital identity services are flexible for everything a business needs to be successful with IoT.

everyday

To create a future we can all trust, individuals, enterprises and governments must be able to rely on smooth yet secure digital interactions. From making online transactions more convenient to securing an ever-increasing number of devices, our trusted digital ID solutions are already an essential part of daily life for millions of people around the world.



*source: Statista

Trusted **digital identity** for
everyone



Trusted digital identity for **consumers**

Financial Institutions

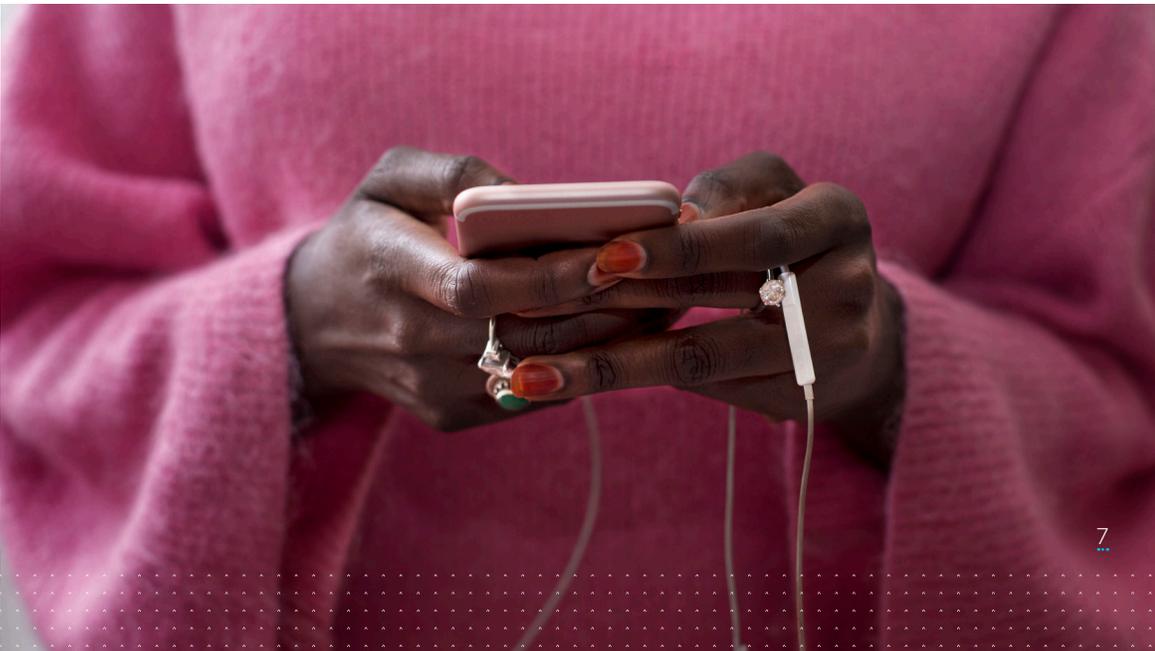
Regulatory changes. Digital transformation. Fierce competition. The rapid evolution of the financial services sector is driven by a number of different forces.

Traditional banks must be able to compete with pure digital players. Doing so means offering customer-focused, mobile-centric services that include simple ID verification and authentication.

These services must be compliant too. Especially with a growing number of rules and regulations like PSD2, and many others, governing everything from payments to anti-money laundering. Tackling fraud remains a huge issue in this sector and digital identity has a key role to play. Now that people are applying for accounts and credit cards online, institutions need to know people are who they say they are without asking them to come into branches.

That is why more than 3,000 financial institutions, retailers and other market players turn to Thales to secure digital and physical transactions.

We provide strong identity verification for customer onboarding. We encrypt payment data between people, merchants and banks. We provide multiple forms of authentication, including biometrics, for accessing digital banking services. And we provide the agile and resilient technical infrastructure to help our customers continue adapting to change.



Trusted **digital identity** for
**secure
financial
services**

Case study:
itsme®

Belgian Mobile Identity scheme - itsme®

itsme® was developed by Belgian Mobile ID, a consortium of Belgium's leading banks and mobile network operators. It was officially recognized by the Belgian government as a way for citizens to connect to numerous online public services, including taxation, pensions and health, as well as online banking and mobile operator services. It provides merchants, government, and financial institutions with strong, multi-factor authentication that is fully compliant with PSD2, GDPR and is certified for eIDAS.

Case study:
La Poste

Digital ID service in France

Docaposte, the digital subsidiary of La Poste (the French national post office), has deployed a strong authentication solution to secure Identité Numérique, La Poste's digital ID service. The security is based on a unique combination of an identifier, a mobile app and a personal authentication code.



Mobile Operators

The mobile sector is undergoing an exciting transformation with 5G offering a network technology with new levels of speed, latency and reach. More and more consumer interactions are happening online – from onboarding and SIM set-up right through to accessing mobile services and device upgrades, all while ensuring data privacy.

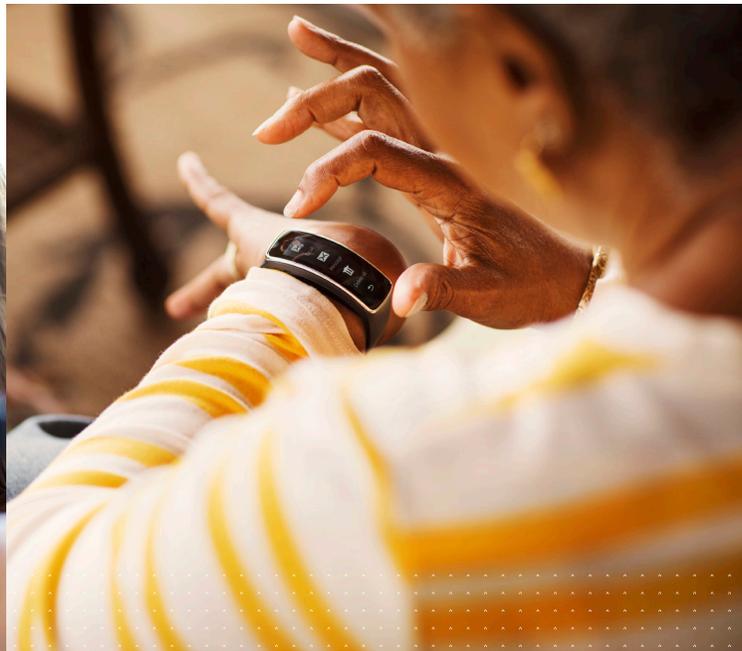
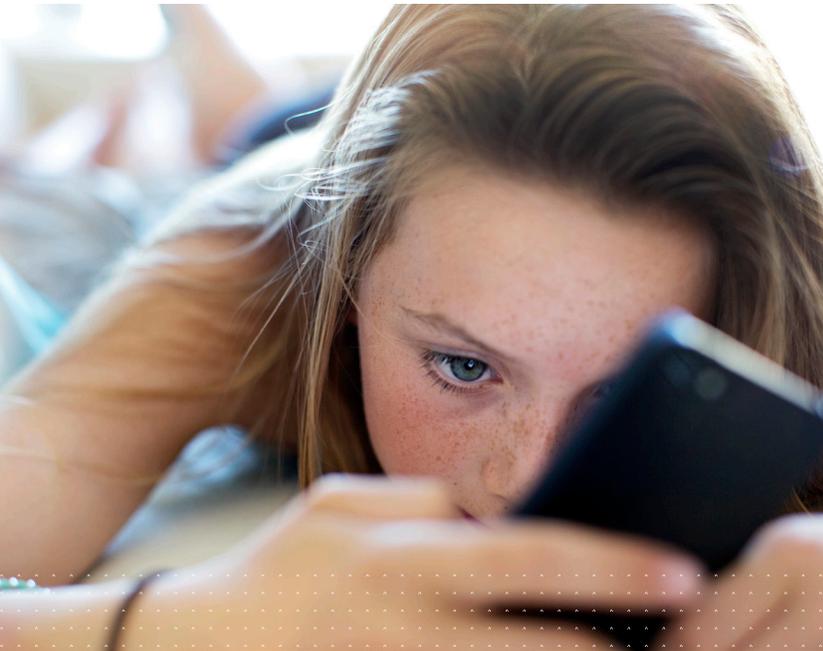
Since the very start of GSM, we've been bringing trust to the mobile ecosystem. Mobile operators rely on us to connect and authenticate millions of users and devices every day. Many people want the convenience of buying the latest smartphone or signing up for a new subscription from the comfort of their homes. Mobile operators need a trusted way of identifying their customers in this digital context. The solution needs to comply with regulations and protect against identity theft.

Our trusted digital identity platform is built to secure the end user on-boarding with ID document verification and biometric identification. This ensures the user is “trusted” because, during the enrolment phase, the user’s identity is checked. This online on-boarding and user authentication then provides secure access to mobile services.

We're also on a mission to build a 5G world we can all trust. Through trusted digital identity for customers and devices, featuring the latest eSIM technology, we offer everything operators need to connect and protect access to cellular networks.

Case study:
MNO

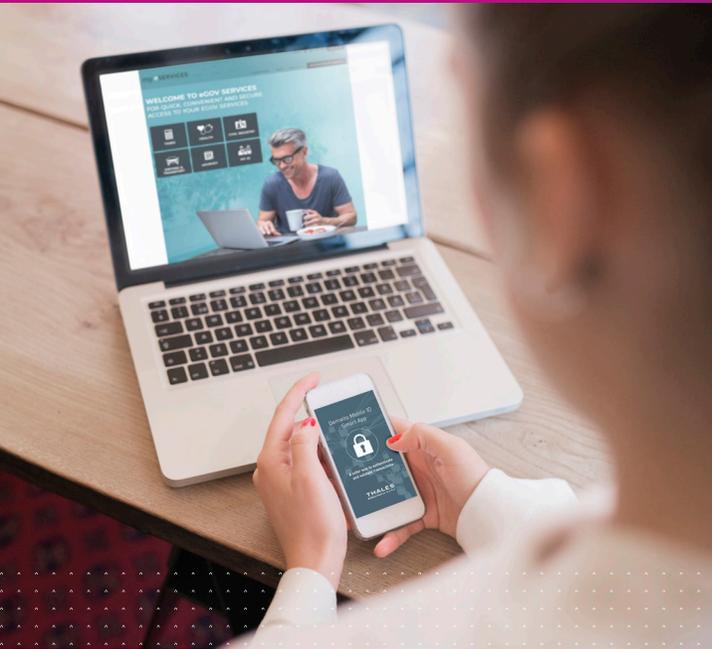
Trusted **digital identity** for
mobile
customers



Identity verification for Asian mobile operator

Mobile operators worldwide are facing identity fraud and have to comply with ID verification regulations for their subscribers. A leading Asian operator has turned to an electronic Know Your Customer (eKYC) experience to minimize the risk in the enrolment process or during online financial transactions. The company has deployed an ID verification process featuring facial recognition and built-in liveness detection to swiftly confirm a subscriber’s identity and grant access to services.

Trusted digital identity protecting citizens' rights



Governments

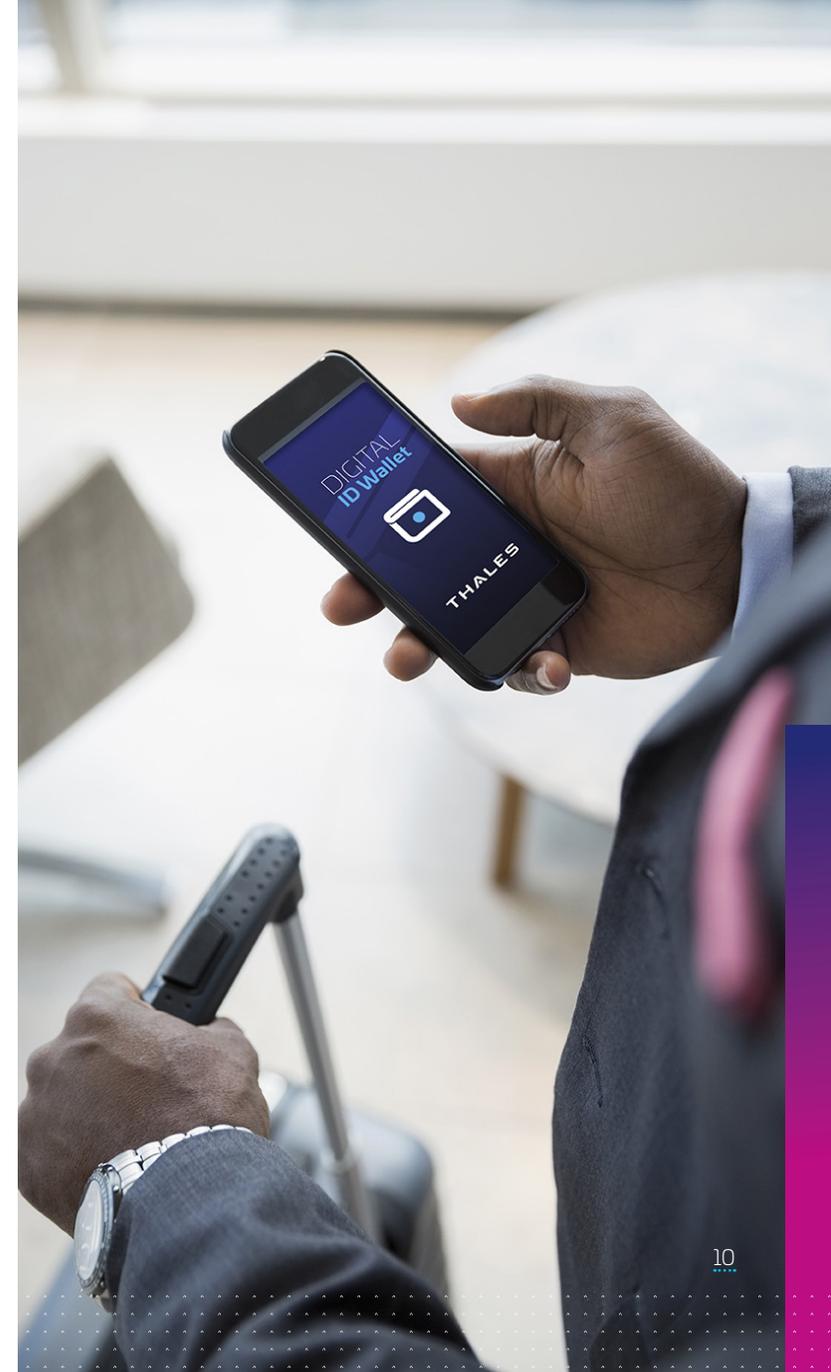
Digital transformation isn't just impacting large enterprises. Its effects can be felt across government bodies and public services. The digitalization of local, regional and national governments has the potential to deliver faster, more convenient services to citizens while delivering organisational efficiencies. And, this digitalisation of public services has been boosted by Covid. Yet all this brings new challenges in terms of data protection, and regulatory compliance.

We believe digital transformation can lead to a safer and more sustainable world. A key part of this are trusted digital IDs to protect peoples' unique identities, citizens' rights, and provide access to services from the public and private sector. Our identity and biometric services allow governments, public bodies and private contractors to keep people, data and systems safe. We are already a leader in highly secure ID documents like passports, identity cards and drivers' licences. And, we've built on this experience to deploy digital ID services and mobile apps to verify people's identities and grant access to online services. These help people prove who they are, both online and in person. But they're not just for public services such as tax declarations or border control. The private sector can also benefit from the infrastructure. A few examples are hotels, car rental companies or concert venues where people might have to prove their identity, their entitlement to drive, show vaccination status or just to confirm their age. With privacy in mind, only the relevant information is shared.

And, around one billion people still don't have an official identity and digital has the potential to bridge the divide while creating a safer, more sustainable world.

Our services are backed by robust software security, data encryption, identification and authentication mechanisms including biometrics - all of which address fraud and public security challenges.

This gives governments and citizens the benefits of digitalisation without compromising their rights or privacy.



Digital ID Wallets

One way to safely store official identities is in a digital wallet on your smart phone. These can be used to hold mobile companions of identity documents from drivers' licenses to national ID cards but also official documents such as boat permits or degree certificates. Citizens get a convenient way to prove their identity or access rights while public agencies benefit from a unique infrastructure & mobile vault for all their digital documents. The wallet encrypts and stores all of the data and is built to comply with local privacy regulations. A range of online onboarding approaches can be integrated including the use of QR codes, selfies and other forms of biometrics. Holders are then free to hire a car if they've forgotten their paper license or provide proof-of-age to get into a concert or bar. Ultimately, the holder manages the privacy of their data only sharing the information required for the purpose of the ID check.

Case studies:

Digital Licence in Queensland, Australia

The all-in-one Digital Licence solution utilises a privacy enhanced app that acts as a secure digital vault to store a wide range of digitalized official documents, starting with the owner's Driver's Licence, Photo Identification Card, Marine Licence and vehicle registration. It delivers ease of access via a smartphone, while ensuring the owners have complete control over their personal data.

Mobile Driver Licenses in Florida

Florida will be the first state in the United States to provide mobile Driver Licenses. Florida residents will be able to apply for new mobile Driver Licenses that are easily accessible on a variety of devices, including smartphones and tablets. These new licenses have the same validity as traditional driver's licenses to verify identity, including proof of age and driving privileges. It also provides an additional role as a strong authentication tool, enabling Floridians to securely prove who they are online for a variety of services.



Trusted digital identity for employees



Enterprise

The increasing use of cloud software has enabled people to work from anywhere. This trend towards remote working was accelerated by COVID. It forced huge numbers of people – from employees to contractors – to access corporate networks from home. This opened the door wider to cyber criminals. With so many employees working away from the office, knowing who is trying to access what on the corporate network is a major concern for IT security teams. Especially when employees still want fast, convenient access to the systems that allow them to get on with their jobs.

We provide enterprises with flexible and scalable access management controls and multi-factor authentication to verify people's identities. Built on the cloud and for the cloud, we deliver convenience and security by enabling the right authentication and single sign-on for employees. Wherever they are, and whatever app they're using, we make sure that your users' identities are protected and that your apps remain secure. Complex organisations can validate employee identities and enforce access policies – all from a single, easy-to-navigate console.

Safe and reliable remote access

Enterprises around the world gain peace of mind that the people accessing corporate systems are who they say they are. In some cases, it is large public organisations like academic medical centres and hospitals that need to prevent unauthorised entry to resources and stop cyber thieves stealing sensitive data. In others, it is major industrial producers that need to provide remote access to employees without authentication downtime or lost productivity. Meeting a wide range of needs, our trusted digital identity for enterprises offers the flexibility to maximise existing authentication investments while providing the most secure remote employee access.

"Security attacks are unrelenting and we view multi-factor authentication as a vital and necessary addition to VUMC's enterprise cybersecurity programme."

**Executive Director of Enterprise Cybersecurity
Vanderbilt University Medical Center, USA**



"The best thing of all is that we have a 100% stable authentication solution. We don't have worry about uptime – the system is always up and running."

IT Manager, Westcon, Norway

Trusted **digital identity** for
everything



Trusted digital identity for the Internet of Things

The Internet of Things has the potential to transform both the way we work and our everyday life. Yet the widespread use of connected devices opens up the potential for cyber-attacks that are hard to manage using manual IT resources.

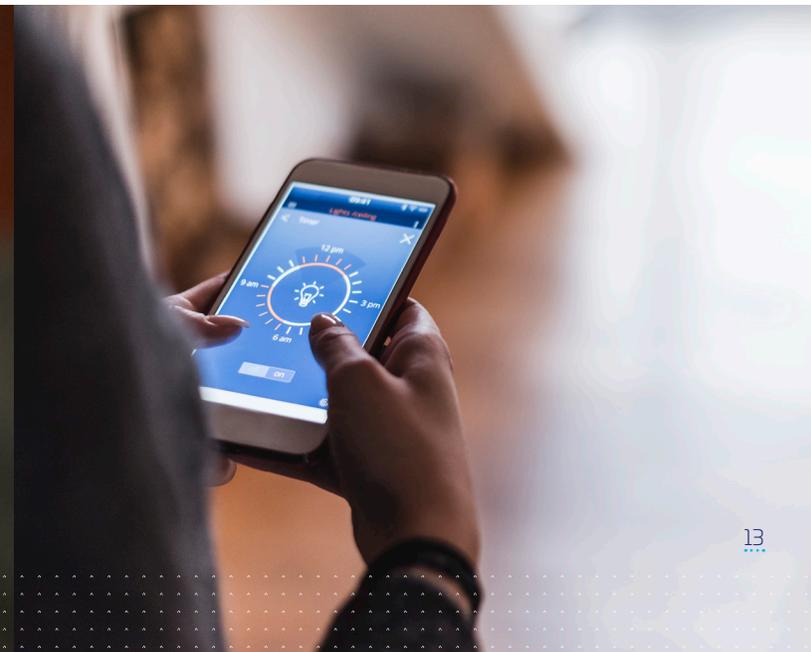
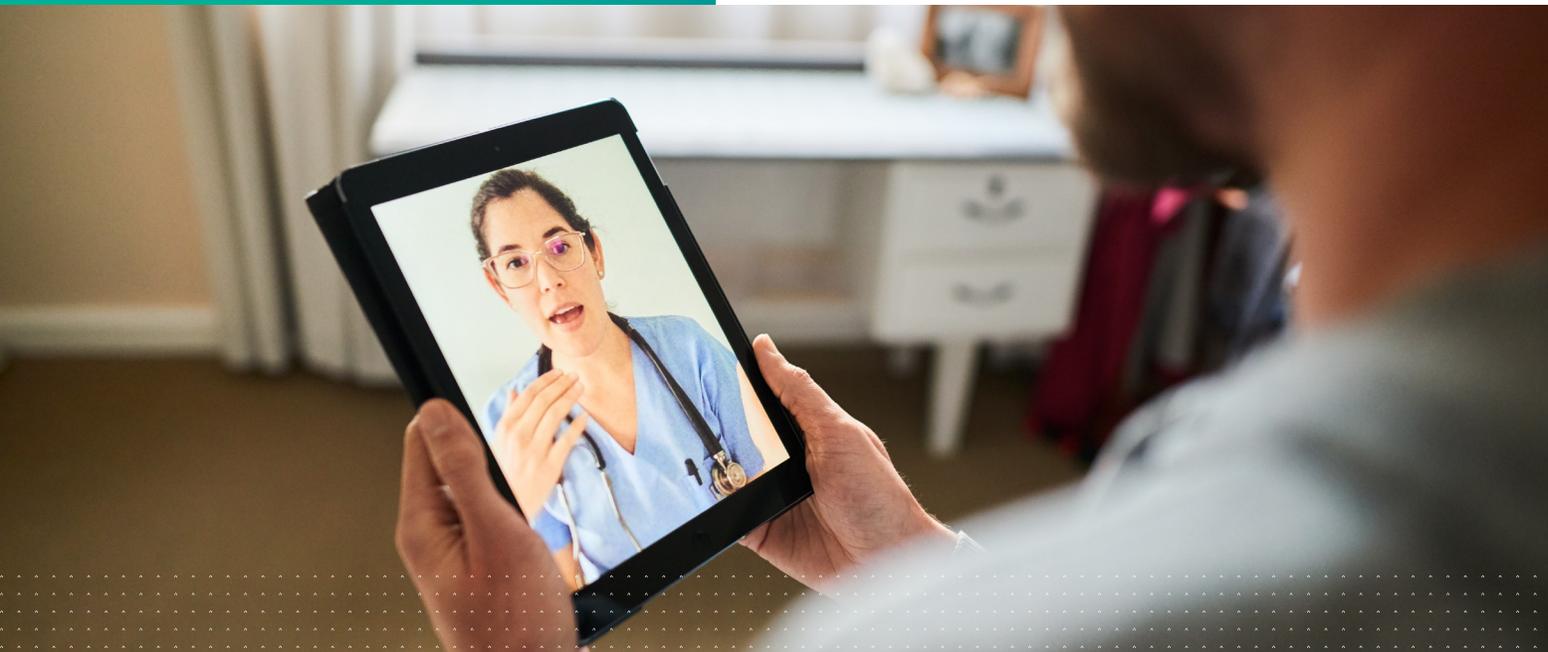
From essential services in healthcare and utilities to consumer devices in connected cars and smart homes, trusted digital identity has become a necessity for protecting people and data. If we look at the field of smart energy, it is important that we have a robust way of trusting the identity of a smart meter. Without this, the devices could be cloned, leading to a range of potential attacks on the wider smart grid network, which is a part of a country's critical infrastructure.

Our trusted identity solutions protect valuable connected devices and secure IoT resources against this type of cloning and malicious access. They provision and store digital IDs and encryption keys, which provide secure mutual authentication between the different parts of the IoT network and provide large-scale credential management for the lifecycle of connected devices.

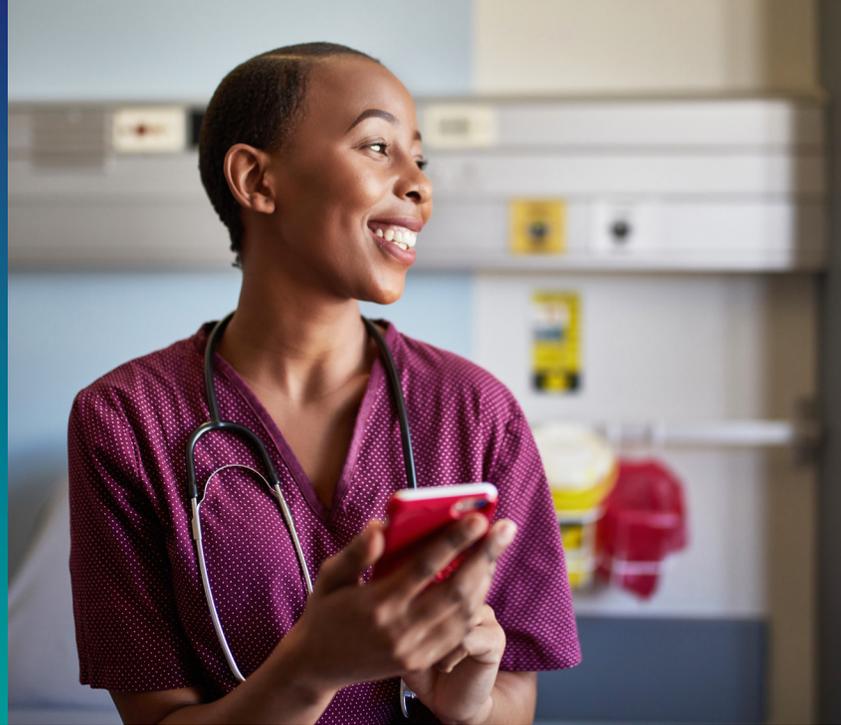
Looking ahead, autonomous cars will need to trust the information coming from other cars and infrastructure in a smart city, at best to avoid traffic jams and at worst accidents. Our secure identity technology ensures data confidentiality and integrity at the source as well as for the user. This creates a trusted IoT infrastructure for device manufacturers and data professionals as well as peace of mind for consumers.

Simpler global IoT deployments

Our solutions reduce the complexity of IoT lifecycle management. The cloud software platform covers connectivity activation, device performance, software updates and trusted identity with secure onboarding. Our Trusted Identity Services leverage years of Thales expertise from delivering more than three million secure devices every year. They streamline unique DI provisioning and maintenance to provide a more efficient, more secure way to remote manage IoT devices. With our Intelligent Cloud Connect LTE Terminal, IoT users get a plug-and-play solution that ensures a consistent, 'out of the box' experience. It simplifies and automates device security as well as the provisioning and connectivity into Amazon Web Services (AWS).



Use cases for trusted IoT



Connected Healthcare

Connected medical devices transmit very sensitive personal information. This must stay private both on the device and in the cloud and should only be accessed by the relevant healthcare professionals. To do this the device needs a unique ID and encryption-based digital signature schemes for messages sent from a device. This avoids cloning or access from illegitimate sources.

Smart Metering

Unprotected smart meters can be hacked to alter consumption data, to gain access to sensitive data, or even to cause physical damage to the global grid. A digital identity in the form of an encrypted key in the meter remotely authenticates and activates key credentials for authorised meters to provide their legitimacy before exchanging data.

Learn more about Digital Identity solutions including:

- Mobile Identity Documents
- Digital Identity Wallets
- Document Verification
- Know Your Customer (KYC)
- Identity Verification
- Biometrics
- Multi-Factor Authentication
- Access Management



THALES
Building a future we can all trust



Trusted digital identity for

**everyone
everything
everyday**

www.thalesgroup.com/digital-id