PROTECT

PESONAL DATA

20 24

SECURITY

Digital Identity

The offers of the trust industry Capacity approach

ACN Allance pour la confiance russérique e

TABLE OF CONTENTS

JEAN-NOËL BARROT, DELEGATED MINISTER'S EDITORIAL4
NTRODUCTION6
EIDAS REGULATORY REVIEW8
THE FRENCH DIGITAL IDENTITY INDUSTRY10
FRANCECONNECT & FRANCECONNECT+12
JEAN-PIERRE BANSARD'S POINT OF VIEW15
HOW TO READ THIS GUIDE ?17
OFFERS BY SEGMENTATION20
CAPACITY OFFERS - FUNCTIONAL SEGMENTATION23
The creation of the digital identity - Subscription to a trusted service24
Registers, management and architecture of attributes and IDP40
The use of digital identity / trusted services50
Personal device58
Service and support70
Digital identity administration76
Safety components82
COMPANY INDEX89
ABOUT ACN112



Credits to: Ministry for Digital Transition and Telecommunications

EDITORIAL

Digital identity

Capacity approach

Jean-Noël Barrot

Minister for Digital Transition and Telecommunications

proliferation of online services and the gradual Connect et Moi ». dematerialisation of administrative procedures. citizens.

and means of authentication.

develop a digital identity solution that prioritises and issuing electronic medical prescriptions. secure practices and fosters a trustworthy digital environment.

Additionally, it is important to consider national electronic identification and trust services, enabling and European sovereignty, especially with the European citizens, residents, and businesses to emergence of private digital identity projects such as those promoted by GAFAM, which offer easy from a European digital identity portfolio. This and secure access to a range of online services.

These issues are central to the French government's of a qualified electronic signature. strategy, which has led to the development of various digital identity solutions in France. These Finally, it is the ambition of several countries that

In the digital age, the concept of digital identity Identité Numérique », and private initiatives, such is becoming increasingly important due to the as « Identité Numérique La Poste » and « Mobile

Just as the passport has become an international The 'POTENTIAL' project also shares this ambition. standard, digital identity will be tomorrow's global The consortium, consisting of 19 Member States, standard. It will have to be ethical and benefit Ukraine, and 144 public and industrial partners, seeks to establish a shared digital identity for all citizens of Europe. The purpose of this project is to A secure digital identity solution should enable test and demonstrate the effectiveness of national citizens to access online services more easily by digital identity solutions and their interoperability reusing previously created logins and passwords, on a European scale. This will be achieved through without having to resort to a multitude of accounts six use cases: accessing electronic public services, opening current, savings and deposit accounts online, registering a telephone line through SIM With the incidence of data leaks, online fraud, card registration, dematerialising driving licences, and identity theft on the rise, it is crucial to providing qualified remote electronic signatures,

> This is also the purpose of the European framework for a digital identity (eIDAS), which aims to develop prove their identity and share electronic documents wallet will provide secure access to a range of public and private services and facilitate the use

include both public initiatives, such as « France have shown great vision in anticipating the

Ukrainian state's digital services. This is also the case of India and its biometric identity programme, It's a major and essential project, I know you're

These examples illustrate the significance of this digital transformation and emphasise the need for Europe to keep pace. Digital identity is a major

future challenges of digital identity and have contemporary challenge that requires a Europeanalready made significant progress in this area. level response. By working together, we can shape For instance, Ukraine has introduced advanced the future of digital identity in Europe, enhance our digital identification measures with its mobile economic independence, and provide our citizens application, Diia, which centralises access to the with a secure and prosperous digital experience.

Aadhaar, which now has almost 1.4 billion users. committed to it, and that I can count on you to work with me on it.



Introduction



"This document demonstrates the breadth, wealth and dynamism of the French digital identity industry, in which the Digital Trust

A NEW ERA OF DIGITAL IDENTITY

THE NEED TO DEPLOY SECURE DIGITAL IDENTITY WALLETS FOR ALL **EUROPEANS**

In recent years, a new form of digital support - economy, and will also ensure the security and electronic identification and authentification but an edifice. can be used to support users in their daily lives, of digital identity.

The revision of the eIDAS regulation will require the state to provide a secure digital identity wallet to all French citizens. This text represents a strategic challenge for the development of the French

which GAFAM and BATX have already begun to the protection of fundamental freedoms. Thanks to deploy - has emerged: the European digital identity a network of high-performance, world-renowned wallet (EUDI wallet). The support is no longer digital trust companies, our country has all the confined to a simple mobile identity application for building blocks and skills needed to build such

whether for remote or face-to-face operations The ease of use and appropriation of digital identity (proving identity, confirming access rights, storing wallets by all private and public players is also a or exchanging documents or attributes, using decisive factor in the success of such a project, various payment methods, accessing trusted digital which will also be a strong factor in digital inclusion services with probative value, etc.). In response, and the development of digital initiatives based on the European Union launched a project to revise these new, highly secure tools. The Alliance pour the eIDAS regulation, with the aim of providing la Confiance Numérique (ACN) has also welcomed all natural and legal persons with a European the initiative launched by the French Ministry digital identity wallet that complies with European of the Interior to join the large-scale European values of security and personal data protection. It pilot «POTENTIAL», aimed at demonstrating enables Europe to retain its sovereignty in terms the interoperability of the wallet with 19 other countries and over 140 public and private partners.

PERSONAL DATA PROTECTION **ENHANCED THROUGH DIGITAL SECURITY CONCERNS OF 2024 OLYMPICS**

functionning their activities.

The 2024 Olympic Games in Paris are an opportunity for supervised experimentation with

It is essential to support users and make them new digital identity solutions. Service providers aware of the potential exposure of their digital and manufacturers of the digital trust alliance identity data to existing risks (identity theft, technologies will adapt to ensure security and online fraud, etc.). Whether used by the private respect for users' public and individual freedoms sector (citizens, businesses) or the public sector in the context of this event. Every actors of the (administrations), the protection of personal French industry are ready to mobilize, alongside and professional data is required for the proper the State and the citizens, to provide France a controlled and trusted cyberspace.

UPDATE OF THE **eIDAS REGULATION**

TOWARDS A EUROPEAN DIGITAL **IDENTITY WALLET**

1. EUROPEAN ELECTRONIC IDENTITY REGULATION phase). Following an initial provisional agreement EIDAS UPDATED TO ADAPT TO MARKET on November 8 2023, an agreement on the eIDAS2 **DEVELOPMENTS IN CYBERSPACE**

Europe. The European regulation eIDAS - electronic quarter of 2024. IDentification And trust Services (published in technology. The use of a wide variety of data in guarantee trust in data transactions. cyberspace is now an integral part of our daily transactions, and has even become inseparable 2. THE DIGITAL IDENTITY WALLET: AN from them.

The proposal to revise the eIDAS regulation (eIDAS 2) aims to expand the existing legal framework The eIDAS 2 regulation requires Member States to meet changing market needs, in particular to make a digital identity wallet available and by establishing reliable and recognized identity free of charge to all citizens and residents of attributes. The revision proposal was published the Union but also to legal entities. A wallet is on June 3, 2021 by the European Commission. designed to be an interoperable tool for electronic The Council of the European Union then adopted identification and authentication, as well as for its general approach on the proposed regulation data management and sharing. It consists of a on December 6, 2022. The European Parliament digital device enabling users to store and manage then published its position on this matter on their identity data (regalian and «extended») in a March 2023, enabling institutional negotiations secure and functional way. with the Council of the EU to begin (trialogue

revision was formalized on December 7 2023 on the basis of a draft text which is scheduled to be Data protection is a central issue in digital vision of put to a plenary vote in the Parliament in the first

2014), in force since 2016, was established to eIDAS 2 provides for the use of a secure, harmonized cover the subject of legal recognition of electronic and interoperable tool: the European Digital interactions, particularly during transactions Identity Wallet (EUDI wallet). On the one hand, between citizens, public players and industrial the wallet will be designed to hold all types of data stakeholders within the European Union. It defined in dematerialized form, as regalian identity data the fundamentals of a common legal framework but also «extended» identity data corresponding for the recognition of digital identity and acts with to everything that can relate to an individual, probative value in digital format. Nevertheless, such as the possession of a driving license or the confinements caused by the COVID 19 a travel document. Secondly, it must enable pandemic have accelerated the dematerialization secure access to services through identification of procedures and increased the use of digital and authentication operations. This tool must

INTEROPERABLE, HARMONIZED AND SECURE

A portfolio prototype is currently being developed The regulation provides a toolbox for an Architecture at the European scale, financed by the European and Reference Framework (ARF). The ARF defines a Commission. The aim is twofold. Firstly, to provide common set of standards, technical specifications, member states with an open-source technical guidelines, security certification requirements reference implementation of the wallet, which and best practices for implementing eIDAS 2. they will be free to use or not for their national Member States are then free to develop their own deployments. Secondly, to validate and refine national portfolios, as long as they comply with the technical specifications that will serve as the technical requirements established by eIDAS a reference for all wallets, thus enabling the 2, thus ensuring its interoperability within the interoperability of this tool in Europe. In order European Union. to achieve this, the wallet is being developed in conjunction with a number of Large Scale Projects 3. TRUST GUARANTEED IN EUROPEAN CYBERSPACE Pilots (LSPs), which are also receiving European funding to define and test different real-life The eIDAS 2 regulation requires wallets to be service providers, public and private bodies, etc.) risk of misuse or alteration of identity or data. Confiance Numérique - ACN). The final technical regulations (EU CSA, EUCC, RGPD...). specifications of the wallet, resulting from these large-scale pilot experiments, will form the toolbox provided for in the draft regulation.

use cases based on the wallet. Four European secured tools guaranteeing a high level of security. consortiums bringing together the relevant The aim is to place trust at the heart of all digital European players (member states, manufacturers, uses, particularly transactions, and to reduce the have been formed to carry out these large-scale The Digital Trust Alliance considers that the digital pilots: POTENTIAL, NOBID, Digital Credential for identity wallet must ensure both (1) a high level Europe (DC4EU) and EU Digital Identity Wallet of security and trust in order to limit the risks of Consortium (EWC). The POTENTIAL consortium identity fraud for the service provider, and (2) a is the one with the most member states (19) high level of protection for the personal data of and partners (over 140), covering 6 use cases: (1) the bearer that it processes. These two conditions electronic government services, (2) bank account are prerequisites for the digital identity wallet to opening, (3) SIM card subscription, (4) electronic be recognized and accepted by everyone, in every signature presumed reliable, (5) mobile driving country of the European Union. Indeed, the trust license and (6) electronic medical prescription. that everyone can place in one or more digital The consortium brings together the majority of the identity wallets is a precondition for trust in all the French digital identity industry, most of whom are digital uses that will follow from them. To achieve members of Digital Trust Alliance (Alliance pour la this, the wallet should comply with European

DIGITAL IDENTITY IN THE DIGITAL TRUST **SECTOR**

Digital identity products and services fall within Digital identity segments within the Digital the industrial scope of Digital Security and Security perimeter: Cybersecurity products/software.

Digital Security covers electronic products and - Identification & Authentification of people: solutions for implementing digital systems to build trust in the outside world. These systems implement secure digital means to build trust in the citizen environment, in particular through identity But also within the field of Cybersecurity products/ management, access management, biometrics, software: transactions, connected objects and vehicles, industrial processes and logistics, transport, - Identity and Access management networks, smart cities, etc. Digital security products are hardware products (smart cards, documents, readers, etc.) or equipment (access management, biometrics, detection, localization, etc.).

- Access control : Full system
- Biometrics / Smart cards / Badges, ID cards, etc. / Vehicle recognition / Anti-counterfeiting

TECHNOLOGY TRENDS

sovereignty, the need to redefine digital at the French level around the deployment of identities also stems from the development the National Electronic Identity Card (CNIe) and of electronic tools and digital transformation FranceConnect, and at the European level around («remote citizenship»). The current norm in France the digital identity wallet project (eIDAS2). remains the simultaneous existence of numerous the user who then manages as he wishes his European players only. other identities derived from the first. The French industrial sector has all the players and skills required for this alternative (secure elements, Identity & Access Management (IAM), integration of solutions, cryptography, biometrics, PVID,

Strongly correlated with the issue of data etc.). The project is beeing shaped since 2022

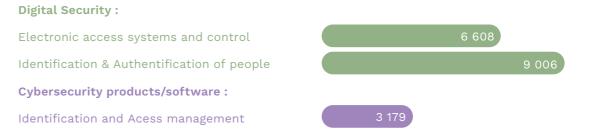
uncorrelated identities, strong (SIM, bank cards, One possibility for the future would be the synergy passports, etc.), substantial (La Poste's digital between the digital identity and the sovereignty, identity), and weak (digital identities issued mainly with the deployment in Europe of a strong digital by American digital players such as GAFA for identity, certified by a trusted public organization e-commerce), with no guarantee of a sovereign and associated with derived identities centered data protection. The alternative is the deployment on the user as well as with connection data of an unique and sovereign strong identity for which are themselves stored in Europe and the government applications and associated with use of which would be conditionally reserved for

KEY FIGURES OF THE INDUSTRY

Size and growth from 2021 to 2022



Workforcer in France in 2022 per segment



Number of companies in France in 2022 per segment





2023 ACN Observatory of digital trust sector



FRANCECONNECT & FRANCECONNECT+

Digital identity

Capacity approach

Focus on the French government's secure and trusted solutions to make it easier for the French to connect to online procedures.



Lauren TRON

Simplifying and securing access to online procedures is the promise of FranceConnect. Launched in 2016, this online identification service offered by the French government has reached more than 40 million users, and its even more secure version: FranceConnect+ dedicated to the most sensitive procedures requiring enhanced security has just reached one million users. An interview with Lauren TRON, FranceConnect partnership manager at the interministerial digital department of the French Ministry for Public Transformation and Civil Service, which created and operates FranceConnect and FranceConnect+.

Q: Could you remind us of FranceConnect's barometer), and 86% find FranceConnect easy to ambitions?

A: Since 2016, FranceConnect has established The target of connecting 1,300 online services itself in the French digital identity ecosystem, via FranceConnect by the end of 2022 has been becoming one of the most widely used online exceeded, with 1,700 online services connected services, with almost 330 million connections by to date. We are continuing our efforts to provide 2022 and over 42 million unique users by July 2023, users with even more online services. results that have far exceeded the targets that had easier and more secure for a maximum number of place? What is the difference with FranceConnect? users to connect to a maximum number of online administrations.

its launch 7 years ago? What has been achieved registered letters. It is also a solution to combat to date?

4 times a year today, compared with 7 million by de formation (CPF). the end of 2020. Moreover, 74% of French people say they trust FranceConnect, according to the Acsel barometer study for French confidence in the digital world in 2022 (1) (+5% on the 2021

use (October 2022).

been set. The aim behind this service is to make it Q: Why was FranceConnect+ created in the first

services, while remaining open and interoperable A: FranceConnect simplifies and secures access to with other European digital identities and services, online procedures. FranceConnect+ is dedicated to and securing the exchange of citizen data between the most sensitive procedures requiring enhanced security, including financial transactions such as opening a bank account, or consulting personal Q: What results has FranceConnect achieved since data such as medical records or electronic fraud attempts and meet the security requirements of these procedures, which is why FranceConnect+ A: In addition to the number of unique users, it has become, since October 2022, the entry key for is interesting to analyze the use of the service, purchasing training on the moncompteformation. almost 20 million French people using it more than gouv.fr platform linked to the Compte personnel



In concrete terms, it works with a reinforced digital identity. two-factor authentication, similar to what users and proceed in complete security.

by the National Agency for Information Systems Republic, Greece, Malta). Security (ANSSI), will soon be available via FranceConnect+.

online pre-admission and Equisign for electronic online services. registered mail. Other online services for healthcare, banking or financial transactions are expected Find out more about FranceConnect: https:// to join FranceConnect + by the end of 2023, in franceconnect.gouv.fr/franceconnect line with the Prime Minister's announcements Find out more about FranceConnect+: https:// on May 9 at the inter-ministerial committee for franceconnect.gouv.fr/france-connect-plus public transformation, dedicated to simplifying Find out more about Interministerial Digital French and combating administrative complexity. gouv.fr/dinum/

Q: What's the latest on FranceConnect's European expansion? What do you see as the future of digital identity?

A: At the end of February 2021, FranceConnect, FranceConnect + and its eIDAS interoperability node obtained ISO 27001 certification, a prerequisite for opening up the European interoperability node. Since then, the node has been gradually opened up, enabling French citizens to access European online services via FranceConnect+ and La Poste

already know for their banking transactions. This breakthrough is the result of the European To date, FranceConnect+ relies on L'Identité Commission's notification in September 2021 of the Numérique La Poste, the system's first partner. French identity scheme, enabling the French eIDAS To authenticate themselves with this service, users node to be opened to other European identities, identify themselves with their cell phone number, thereby facilitating European citizens' access to receive a notification on their smartphone via the European online services by connecting via their application, enter the secret code they have chosen national identity services, FranceConnect being the one for the French. Since July 2023, the eIDAS node has been open in 9 countries (Belgium, Spain, Other digital identities, currently being qualified Luxembourg, Denmark, Portugal, Sweden, Czech

France Identité Numérique, the digital identity linked to the electronic identity card, will be In fact, we've just reached the million-user mark. integrated into FranceConnect and FranceConnect + by the end of 2023. French citizens will thus be To date, 3 online services are available on able to use their ID card via their smartphone to FranceConnect +: Mon compte formation, APHP for connect to FranceConnect and FranceConnect +

and improving administrative procedures for the Department (DINUM): https://www.numerique.

(1) : https://www.acsel.eu/wp-content/ uploads/2022/02/ACSEL-Barometre-Confiance-9eme-ED-Synthese.pdf

Reinforcing the security of the most sensitive procedures, such as training or receiving assistance, is a priority for Stanislas Guerini, the French Minister for Transformation and the Civil Service, to ensure that public services meet the needs of the French people.



POINT VIEW

Jean-Pierre BANSARD

Senator for French citizens living outside France Member of the Senate Economic Committee Grand Officer of the Legion of Honor

Few things have revolutionized our lives as much Constitutional Council on the basis of internet our way of communicating and talking to each necessary for double authentication. other, has been turned upside down. The State has undergone profound reform to integrate the To ensure that e-voting becomes an even more every day.

funds (for which advances in digital identity are us. It's up to us to seize it! necessary). As well as another aspect, far more central and less well known in France: electronic voting. First used in the 2014 elections, suspended on the eve of the 2017 legislative elections - due to risks of intrusion - it was used again in 2021, then last year for the legislative elections.

Digital technology is also changing our relationship with democracy. By enabling French citizens living far from a French consulate to express their preferences, their relationship with France is also changing. Yet the questions raised are numerous and the errors possible, as demonstrated by the cancellation of two legislative elections by the

- and as quickly - as digital technology. With voting malfunctions in January 2023, notably due uncommon speed, every aspect of our economy, to the non-reception of SMS in certain countries,

benefits of technology, and the potential of digital powerful tool, perhaps to the point where it technology goes far beyond what we perceive becomes widespread one day, the French digital industry needs to work on it. The two voting platforms used to date are Spanish and Swiss. I The French population living abroad, whom I have no doubt, therefore, that this catalog contains represent, are perhaps the ones who are most many nuggets capable of taking up this subject. aware of the advantages - and disadvantages - in The future of our democracy, where voter turnout, all their dealings with the administration: making particularly among young people, has fallen to online appointments at the consulate, requests for particularly worrying levels, may well be at stake. birth certificates, proof of life required for pension Collectively, we still have a lot of work ahead of



HOW TO READ THIS GUIDE?

This guide has been designed to meet the needs of any entity wondering about digital identity and looking for the offerings available in this field. To ensure maximum readability for the reader, the digital identity process has been segmented into seven stages: creation, attributes, trusted service, personal device, service and support,

NATURE OF THE OFFER





OFFER CRITERIA

regarding the targets adressed by the offers listed was integrated. We decided to separate these targets into four categories.







allows you to cross-reference the segments, the descriptions of the offers (part 2) and general nature of the offer and the criteria, for a dynamic presentations of the companies offering them reading according to the most relevant criteria (part 3).

How to read this guide?

Digital identity
Capacity approach

HOW TO READ THIS GUIDE?



IDENTITY CREATION & SUBSCRIPTION TO A TRUSTED SERVICE - ENROLMENT AND IDENTITY VERIFICATION IN PROXIMITY/FACE-TO-FACE OR REMOTELY

Implementation of the components and services needed to establish the applicant's identity, i.e. collection of identity information (identity document, biometrics, civil status, etc.) and verification of the identity and link with the applicant (biometric deduplication, detection of living persons, verification of the authenticity of a document, etc.). This step is a prerequisite for any use of a digital identity or trusted service of any kind.

- Proximity collection devices
- Capture and verification of credentials or source documents: validity, authenticity via authentication of physical security and/or chip and/or visible electronic stamp/integrity
- Capture and verification of biometric data and link between credential and bearer, with live detection
- Verification of uniqueness/deduplication



REGISTERS, MANAGEMENT AND ARCHITECTURE OF ATTRIBUTES AND IDPS (IDENTITY AND OTHER)

An identity management system or a trusted service relies on various data management infrastructures and digital credentials.

- PKI
- Blockchain
- Verifiable registry technologies and products (shared, distributed, DLT etc. ...)
- Civil registry (PID)
- Other attribute registers
- Interfacing different building blocks
- IDP
- Solution provider PIMS Privacy Identity Management System

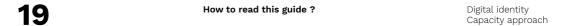
Capture, notarization and management of consents / Management of access, modification, deletion and revocation rights / Privacy control tower user interface



TRUSTED SERVICES

The eIDAS regulation regulates trusted services such as the issuance of digital identities and their use for strong authentication of natural and legal persons, electronic signatures (including verification, storage and archiving), and electronic registered mail.

- eIDAS trust service providers of electronic attestations ((Q)EAA), Provider of qualified certificates and validation of qualified certificates
- eIDAS provider of electronic (ledgers)
- Digital safe in accordance with the French Law for a digital republic (LRN)
- Digital archiving as defined by eIDAS
- Electronic registered mail
- Electronic signature and verification
- Signature verification





PERSONAL DEVICE

A solution that enables strong authentication for service access, electronic signature or encryption to be performed locally (on the client workstation). Their exclusive use is based on authentication factors (possession, knowledge, who I am / or what I do / or their combination (MFA, 2FA, 3FA...)).

- Personal devices as defined by eIDAS
- Means of electronic identification (MEI) / Wallet EUDI
- Authentication means and factors

Biometrics: solutions and software for biometric authentication (e.g. Match On Card), products (e.g. sensors) / solutions and software (e.g. Match On Card) for authentication / Hardware solution (FIDO key, etc.) / Intangible solution (Front and Backend application)

- Other authentication factors
- Electronic credentials (possession, biometrics) / Visible electronic stamp (CEV)
- Electronic signature QSCD qualified smart card



SERVICE AND SUPPORT

Services covering a broad spectrum of know-how and expertise around the specific challenges of digital trust and beyond: Support for service qualification / Certification / RGPD compliance / Labeling & homologation / development, design, project management and contracting, training, consulting, expertise.

- Certification
- Qualification
- Audit
- DPIA
- Homologation - Certification

- Remediation plan
- Consulting and expertise
- Training
- Route, UX, design
- Project ownership, operational assistance, project/program management...



DIGITAL IDENTITY ADMINISTRATION

Digital identity administration can be carried out according to different models and associated tools, depending on the needs of each use case (BtoC, BtoBtoC, BtoB, GtoC, GtoB, etc.).

- Tools for centralized administration
- CMS / IAM
- Tools for user-centric administration
- SSO / CIAM
- Tools for decentralized administration with identity federation
- Tools for decentralized, distributed SSID administration with or without DLT/blockchain



SAFETY COMPONENT

Includes components and ancillary services, implemented on the personal device used or on a central server. These components can be hardware / software / cryptographic / remote services / management services.

- Secure hardware provider
- Reader
- HSM
- Provider of cryptographic solutions / protocols to protect privacy
- Mobile device components for secure storage of keys or content
- Tools required for electronic signatures
- Biometric sensors

OFFERS BY SEGMENTATION

			Ju				•
	Identity creation & subscription to a trusted service	Registers, management and architecture of attributes and IDPs	Trustworthy service	Personal device	Service and support	Digital identity ad- ministration	Safety component
A3BC				Pages: 58			
BLOOO		Pages: 40, 43, 44, 45, 46,48					
ARCHIPELS			Pages: 52, 55, 57			Pages:	
ADVANCED TRACK AND TRACE			Pages: 54, 55 56, 57				
CERTIGNA	Pages: 27, 34		Pages: 50, 52, 53, 56				
CHAMBERSIGN	Pages: 28		Pages:				
DOCAPOSTE	Pages: 24, 28			Pages: 58, 62	Pages : 70, 71		
EVIDEN		Pages:	Pages: 54		Pages: 71, 73	Pages: 76, 78, 79	Pages: 84
ID3 TECHNOLOGIES	Pages: 24, 29, 35, 38						
IDAKTO	Pages:			Pages:		Pages : 77	



Product / Software

VSE: SME ISE LA LC GA

OES
OVI

							0
	Identity creation & subscription to a trusted service	Registers, management and architecture of attributes and IDPs	Trustworthy service	Personal device	Service and support		Safety component
IDEMIA	Pages: 25, 29, 37, 38	Pages: 41, 45, 46		Pages : 59, 60, 62, 63 66, 68	Pages: 73		
IN GROUPE	Pages: 25, 32, 35	Pages: 41, 42, 49	Pages:	Pages:		Pages:	
MEROX	Pages:						
NEOWAVE				Pages: 60, 63, 65, 68			Pages:
ORANGE BUSINESS	Pages:						
SHAREID	Pages: 26, 33, 37			Pages: 65		Pages:	
SOPRA STERIA	Pages:				Pages: 72, 74		
STMICROELECTRONICS							Pages: 82, 85, 86
SYSTANCIA				Pages: 61, 64, 65, 67		Pages: 76, 78	
THALES	Pages: 31, 36, 37, 39			Pages: 61, 65, 69			
WORLDLINE		Pages: 43, 47, 48					

CAPACITY OFFERS

FUNCTIONAL SEGMENTATION

THE CREATION OF THE DIGITAL IDENTITY - SUBSCRIPTION TO A TRUSTED SERVICE





ID360





A single hub for all remote identity verification solutions • A global service developed by design to integrate all means of identification, whether French or international, for individuals and organizations, with various levels of security. • A service that enables all users to check their identity, via a French or a foreign Electronic Identification Mean, or via online paths based on ID check and facial video. • A platform that collect and verify all types of documents (address proof, bank details, tax documents, etc.). • And also integrates solutions from Certinomis, the certification authority that secures electronic exchanges • An admin panel and single API integration for all your business processes.





BIOSEAL / VDS



BioSeal is a global and interoperable solution to certify and authenticate all types of products and documents, making them tamper-proof. Thanks to instant and local verification, it helps to fight against fraudulent falsification of all types of documents and to verify the identity of people thanks to privacy-friendly biometric recognition technology.

Bioseal - Use Cases

Capacity offers

IDEMIA



ENROLMENT SOLUTIONS







Enrollment is a critical step in creating a solid and reliable physical or digital identity. IDEMIA offers a complete range of capture and verification solutions based on multibiometrics (face, fingerprints and iris): application system, suite of biometric devices such as high-definition cameras (compliant with ICAO recommendations), multi-functional mobile tablets, fingerprint capture devices and selfservice kiosks. To complete the offer, IDEMIA provides an online preregistration portal that enables citizens to save time when they renew their identity documents at administrative offices.

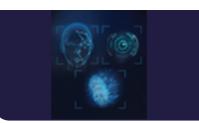
THALÈS



ENROLMENT SOLUTIONS







Thales relies on trusted biometrics to provide solutions which allow government agencies to be more effective at solving crimes, preventing fraud in elections or public services, securing national borders or protecting identities, etc. With 30 years of expertise in biometric technology, Thales offers a comprehensive range of products and services including fingerprint, face and iris recognition, enabling it to help governments and agencies throughout the world to ensure citizens' safety. These technologies may be used during enrollment, identity checks or to access an online service.

IN GROUPE







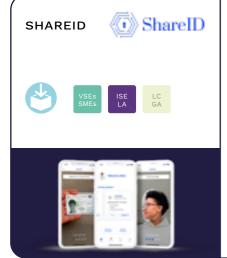




TAME3S enables the rapid, secure acquisition of civil status and biometric data to issue a physical and/or digital identity. The device records the applicant's biometric data (face, fingerprints, iris, signature) via an ergonomic console equipped with sensors, enrolment software and real-time ICAO quality control. TAME3S complies with the most stringent security, quality and data protection standards, and ensures traceability of operations. 4 formats: fixed or mobile stations, self-service kiosks, smartphone enrolment Apps.

26 Capacity offers





SHAREID

ShareID offers various trusted digital SaaS services:

1. Doc IDV: Enables the verification of the authenticity of ID documents from more than 120 countries, with a precision level of up to 99.9%. 2. Full IDV: Integrates the Doc IDV service and enhances it by verifying the user's liveliness and document ownership. This service is available with or without operators.

Digital identity

Capacity approach

3. MFA 3.0 (Multi-Factor Authentication): Strong authentication tied to government-issued IDs. It integrates the Full IDV service to issue a reusable digital identity without storing the users' personal or biometric data. Future interactions only require a simple smile to replicate the equivalent of a real-time identity check.



CAPTURE AND VERIFICATION OF CREDENTIALS OR SOURCE DOCUMENTS: VALIDITY, AUTHENTICITY VIA AUTHENTICATION OF PHYSICAL SECURITY AND/OR CHIP AND/OR VISIBLE ELECTRONIC STAMP/INTEGRITY





CERTIGNA VERIF ID

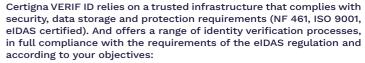














- Identification via 100% video stream and proof of life (ISO / IEC 19575 biometric checks), validation of proof of registration and backoffice verification by certified agents.
- Digital identification via a qualified personal certificate, issued by a certification authority such as Certigna.



















Based on a 100% video pathway, enabling both verification of ID authenticity and facial biometrics, thus ensuring proof of life. At the end of this onboarding phase, the user acquires a reusable digital identity that can be used at any time to access the associated service.





CAPTURE AND VERIFICATION OF CREDENTIALS OR SOURCE DOCUMENTS: VALIDITY, AUTHENTICITY VIA AUTHENTICATION OF PHYSICAL SECURITY AND/OR CHIP AND/OR VISIBLE ELECTRONIC STAMP/INTEGRITY



PROFESSIONAL DIGITAL IDENTITY - CHAMBERSIGN





Created in 2000 by the French Chamber of Commerce and Industry and CCI France, ChamberSign France is a Trust Service Provider. ChamberSign provide digital certificates for people and / or companies and they comply with the various RGS, elDAS and ETSI regulations. ChamberSign France guarantee the professional digital identity (individuals or legal entities represented by an individual). As a Certification Authority, ChamberSign is responsible for managing the lifecycle management of the Digital IDs of certificate holders and users. The service is developed, designed and hosted in France.



ID360

A single hub for all remote identity verification solutions • A global service developed by design to integrate all means of identification, whether French or international, for individuals and organizations, with various levels of security. • A service that enables all users to check their identity, via a French or a foreign Electronic Identification Mean, or via online paths based on ID check and facial video. • A platform that collect and verify all types of documents (address proof, bank details, tax documents, etc.). • And also integrates solutions from Certinomis, the certification authority that secures electronic exchanges • An admin panel and single API integration for all your business processes.





BIOSEAL / VDS







BioSeal is a global and interoperable solution to certify and authenticate all types of products and documents, making them tamper-proof. Thanks to instant and local verification, it helps to fight against fraudulent falsification of all types of documents and to verify the identity of people thanks to privacy-friendly biometric recognition technology.

IDEMIA



ENROLMENT SOLUTIONS







Enrollment is a critical step in creating a solid and reliable physical or digital identity. IDEMIA offers a complete range of capture and verification solutions based on multibiometrics (face, fingerprints and iris): application system, suite of biometric devices such as high-definition cameras (compliant with ICAO recommendations), multi-functional mobile tablets, fingerprint capture devices and self-service kiosks. To complete the offer, IDEMIA provides an online preregistration portal that enables citizens to save time when they renew their identity documents at administrative offices.

MEROX











Merox is an «all-in-one» French SaaS platform for tracking, monitoring, domain compliance and technical protocol implementation assistance (DMARC, SPF, DKIM, BIMI, DNSSEC, CAA, MTASTS...). Main features: Mapping and control of the entire DNS environment Analysis of DMARC reports Monitoring and verification of DNS entries Blacklist monitoring Complete toolbox to help implement security protocols Security alerts: potential attacks and unwanted changes on your domains Monitoring of lookalike domains Benefits: • Control your entire DNS environment • Prevent phishing & spoofing • Improve your security posture & reduce cyber-insurance costs • Make your brand stronger & increase email deliverability and marketing KPIs.



CAPTURE AND VERIFICATION OF CREDENTIALS OR SOURCE DOCUMENTS: VALIDITY, AUTHENTICITY VIA AUTHENTICATION OF PHYSICAL SECURITY AND/OR CHIP AND/OR VISIBLE ELECTRONIC STAMP/INTEGRITY



LIVE IDENTITY WALLET

Live Identity Wallet, provides to companies a solution to build trust ecosystem with their partners. It's a self sovereign identity solution for natural and legal person or objects - Share data in complex ecosystems - Simplify partners registration - Reduce the cost of transaction- Live Identity Wallet manage verifiable credential compliant with W3C. Complete solution compatible with Blockchain or classic registry (Alastria, ABF, ITN, PKI, LDAP etc). Supporting OIDC, OIDC4VP and SIOP protocols, you can store, send and verify information or transactions.



LIVE IDENTITY VERIFY

The strong increase in identity fraud on the web in recent years makes the verification of identity data essential for many actors present on the Internet. This approach may be considered tedious and intrusive for Internet users. In France, one solution stands out, coming from a common initiative by the telephone operators. This is the Live Identity Verify offer, to simplify and secure digital journeys, based on already verified and qualified operator data. The offer is a set of additional and independent functionalities making it possible to verify the digital identification procedures and the consistency of the data declared by the user.

SOPRA STERIA sopra steria









CAPITOLE

Capacity offers

CAPITOLE is a sovereign application designed and created by our teams to meet the mobile biometric collection needs of homeland security forces. Our application enables alphanumeric and multibiometric capture (up to 3 types of biometric: face, fingerprint and iris). Our application is hardware agnostic in terms of both mobile terminals (phone, classic tablet, all-in-one tablet) and biometric capture devices. CAPITOLE leaves you free in the choice of equipment, to meet your exact needs and a wide range of use cases (identity control, border control, refugee claim, access control, mobile brigades).

THALÈS



ENROLMENT SOLUTION







Thales provides end-to-end biometric enrollment services and solutions which are used for both entry and verification in national registers. Enrollment is a crucial step in order to guarantee a secure and reliable register of the population and deploy a legal identity infrastructure. These solutions are based on the reading and verification of official identity documents or connection to databases. Biometrics captures characteristic attributes on faces, fingerprints and the iris. Our comprehensive offer includes a wide range of fixed or mobile equipment, such as biometric scanners – for fingerprint, face and iris capture, enrollment kiosks, or simply mobile solutions on smartphones.

THALÈS



BIOMETRIC SOLUTIONS







Thales relies on trusted biometrics to provide solutions which allow government agencies to be more effective at solving crimes, preventing fraud in elections or public services, securing national borders or protecting identities, etc. With 30 years of expertise in biometric technology, Thales offers a comprehensive range of products and services including fingerprint, face and iris recognition, enabling it to help governments and agencies throughout the world to ensure citizens' safety. These technologies may be used during enrollment, identity checks or to access an online service.



CAPTURE AND VERIFICATION OF CREDENTIALS OR SOURCE DOCUMENTS: VALIDITY, AUTHENTICITY VIA AUTHENTICATION OF PHYSICAL SECURITY AND/OR CHIP AND/OR VISIBLE ELECTRONIC STAMP / INTEGRITY





IN WALLET







IN Wallet is a smartphone-based digital identity solution, derived from a root identity (from an identity provider or physical credential), or from self-enrollment, for secure access to digital services. In Wallet is available for both professional and consumer use, and can address all eIDAS identity levels. As a «Security and Privacy by design» solution, identity data and services associated with In Wallet remain under the user's control, and are never stored in a central database. In Wallet relies on familiar experiences to facilitate user adoption (Smartphone GUI, PIN code).

IN GROUPE



TAME 3 S







TAME3S enables the rapid, secure acquisition of civil status and biometric data to issue a physical and/or digital identity. The device records the applicant's biometric data (face, fingerprints, iris, signature) via an ergonomic console equipped with sensors, enrolment software and real-time ICAO quality control. TAME3S complies with the most stringent security, quality and data protection standards, and ensures traceability of operations. 4 formats: fixed or mobile stations, self-service kiosks, smartphone enrolment Apps.

Capacity offers Digital identity Capacity approach

SHAREID



SHAREID









1. Doc IDV: Enables the verification of the authenticity of ID documents from more than 120 countries, with a precision level of up to 99.9%. 2. Full IDV: Integrates the Doc IDV service and enhances it by verifying the user's liveliness and document ownership. This service is available with or without operators.

ShareID offers various trusted digital SaaS services:

3. MFA 3.0 (Multi-Factor Authentication): Strong authentication tied to government-issued IDs. It integrates the Full IDV service to issue a reusable digital identity without storing the users' personal or biometric data. Future interactions only require a simple smile to replicate the equivalent of a real-time identity check.

IDAKTO



IDCLUSTER









We offer the solution to go from physical identity to reusable digital identity. We help states to build a solid foundation for trust, enabling digital transformation. IDCluster provides a platform (Public or Private Cloud) and citizen applications on mobile devices, ensuring complete, transparent orchestration of the digital identity lifecycle. (KYC, SSO, MFA, CIAM, Wallet) With IDCluster, governments (e.g. Morocco and France) can offer a Secure, Reliable, and Inclusive Digital Identity, protecting personal data of their citizens. Service providers can identify and authenticate their users with assurance and without friction.



CAPTURE AND VERIFICATION OF BIOMETRIC DATA AND THE LINK BETWEEN THE CARD AND ITS HOLDER, WITH LIVE DETECTION

CERTIGNA















Certigna VERIF ID relies on a trusted infrastructure that complies with security, data storage and protection requirements (NF 461, ISO 9001, eIDAS certified). And offers a range of identity verification processes, in full compliance with the requirements of the eIDAS regulation and according to your objectives:

Digital identity

Capacity approach

- Automated checks of ID documents from over 200 countries,
- Identification via 100% video stream and proof of life (ISO / IEC 19575 biometric checks), validation of proof of registration and backoffice verification by certified agents.
- Digital identification via a qualified personal certificate, issued by a certification authority such as Certigna.











identity that can be used at any time to access the associated service.

CERTIGNA DIGITAL ID



Based on a 100% video pathway, enabling both verification of ID authenticity and facial biometrics, thus ensuring proof of life. At the end of this onboarding phase, the user acquires a reusable digital





Capacity offers

BIOSEAL / VDS









Bioseal - Use Cases



BioSeal is a global and interoperable solution to certify and authenticate all types of products and documents, making them tamper-proof. Thanks to instant and local verification, it helps to fight against fraudulent falsification of all types of documents and to verify the identity of people thanks to privacy-friendly biometric recognition

IN GROUPE



IN WALLET







IN Wallet is a smartphone-based digital identity solution, derived from a root identity (from an identity provider or physical credential), or from self-enrollment, for secure access to digital services. In Wallet is available for both professional and consumer use, and can address all eIDAS identity levels. As a «Security and Privacy by design» solution, identity data and services associated with In Wallet remain under the user's control, and are never stored in a central database. In Wallet relies on familiar experiences to facilitate user adoption (Smartphone GUI. PIN code).

IN GROUPE











TAME3S enables the rapid, secure acquisition of civil status and biometric data to issue a physical and/or digital identity. The device records the applicant's biometric data (face, fingerprints, iris, signature) via an ergonomic console equipped with sensors, enrolment software and real-time ICAO quality control. TAME3S complies with the most stringent security, quality and data protection standards, and ensures traceability of operations. 4 formats: fixed or mobile stations, self-service kiosks, smartphone enrolment Apps.





CAPTURE AND VERIFICATION OF BIOMETRIC DATA AND THE LINK BETWEEN THE CARD AND ITS HOLDER, WITH LIVE DETECTION

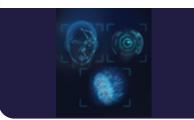
THALÈS











Thales relies on trusted biometrics to provide solutions which allow government agencies to be more effective at solving crimes, preventing fraud in elections or public services, securing national borders or protecting identities, etc. With 30 years of expertise in biometric technology, Thales offers a comprehensive range of products and services including fingerprint, face and iris recognition, enabling it to help governments and agencies throughout the world to ensure citizens' safety. These technologies may be used during enrollment, identity checks or to access an online service.

THALÈS









DIGITAL IDENTITY WALLET



Thales' Digital ID Wallet represents the next generation of Mobile ID. Governments can call upon a platform of digital identity services for complete management of the digital identity lifecycle from the identification and registration of citizens through to the creation of a trusted digital identity, with strong authentication, citizen's electronic signature, and connection to eService providers. In addition to being extremely convenient, the Digital ID Wallet gives citizens total control over their data, with the freedom to decide exactly what information they want to share, with whom and when.





ENROLMENT SOLUTIONS







Enrollment is a critical step in creating a solid and reliable physical or digital identity. IDEMIA offers a complete range of capture and verification solutions based on multibiometrics (face, fingerprints and iris): application system, suite of biometric devices such as high-definition cameras (compliant with ICAO recommendations), multi-functional mobile tablets, fingerprint capture devices and self-service kiosks. To complete the offer, IDEMIA provides an online preregistration portal that enables citizens to save time when they renew their identity documents at administrative offices.

THALÈS



ENROLMENT SOLUTION







Thales provides end-to-end biometric enrollment services and solutions which are used for both entry and verification in national registers. Enrollment is a crucial step in order to guarantee a secure and reliable register of the population and deploy a legal identity infrastructure. These solutions are based on the reading and verification of official identity documents or connection to databases. Biometrics captures characteristic attributes on faces, fingerprints and the iris. Our comprehensive offer includes a wide range of fixed or mobile equipment, such as biometric scanners – for fingerprint, face and iris capture, enrollment kiosks, or simply mobile solutions on smartphones.

SHAREID

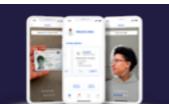












ShareID offers various trusted digital SaaS services:

1. Doc IDV: Enables the verification of the authenticity of ID documents from more than 120 countries, with a precision level of up to 99.9%.
2. Full IDV: Integrates the Doc IDV service and enhances it by verifying the user's liveliness and document ownership. This service is available with or without operators.

3. MFA 3.0 (Multi-Factor Authentication): Strong authentication tied to government-issued IDs. It integrates the Full IDV service to issue a reusable digital identity without storing the users' personal or biometric data. Future interactions only require a simple smile to replicate the equivalent of a real-time identity check.





BIOSEAL / VDS





Bioseal - Use Cases

BioSeal is a global and interoperable solution to certify and authenticate all types of products and documents, making them tamper-proof. Thanks to instant and local verification, it helps to fight against fraudulent falsification of all types of documents and to verify the identity of people thanks to privacy-friendly biometric recognition technology.













ENROLMENT SOLUTIONS

Enrollment is a critical step in creating a solid and reliable physical or digital identity. IDEMIA offers a complete range of capture and verification solutions based on multibiometrics (face, fingerprints and iris): application system, suite of biometric devices such as high-definition cameras (compliant with ICAO recommendations), multi-functional mobile tablets, fingerprint capture devices and self-service kiosks. To complete the offer, IDEMIA provides an online pre-registration portal that enables citizens to save time when they renew their identity documents at administrative offices.

Capacity offers Digital identity
Capacity approach

THALÈS



ENROLMENT SOLUTIONS







Thales provides end-to-end biometric enrollment services and solutions which are used for both entry and verification in national registers. Enrollment is a crucial step in order to guarantee a secure and reliable register of the population and deploy a legal identity infrastructure. These solutions are based on the reading and verification of official identity documents or connection to databases. Biometrics captures characteristic attributes on faces, fingerprints and the iris. Our comprehensive offer includes a wide range of fixed or mobile equipment, such as biometric scanners – for fingerprint, face and iris capture, enrollment kiosks, or simply mobile solutions on smartphones.

THALÈS



BIOMETRIC SOLUTIONS







Thales relies on trusted biometrics to provide solutions which allow government agencies to be more effective at solving crimes, preventing fraud in elections or public services, securing national borders or protecting identities, etc. With 30 years of expertise in biometric technology, Thales offers a comprehensive range of products and services including fingerprint, face and iris recognition, enabling it to help governments and agencies throughout the world to ensure citizens' safety. These technologies may be used during enrollment, identity checks or to access an online service.

REGISTERS, MANAGEMENT AND ARCHITECTURE OF ATTRIBUTES AND IDPS (IDENTITY AND OTHER)





IDENTITY AND DIGITAL TRUST CONSULTING AND SUPPORT

The «Identity and Digital Trust Consulting and Support» offering by Blooo guides you through successful digital transformation based on tailored solutions that comply with upcoming standards. Leveraging our expertise in strategic positioning and comprehensive understanding of the European trusted digital ecosystem, we assist you in securely managing digital identity, protecting data, and establishing reliable trust mechanisms. Together, we build a robust digital environment ensuring confidentiality, integrity, and authenticity of information. Trust our experienced team to secure your digital future and achieve your strategic goals.







IDNOMIC PKI





Companies committed to digital transformation need to be ready to protect themselves against a wide range of potential threats through enhanced identity and data security. With IDnomic PKI, Eviden offers a complete, highly secure solution that is simple to deploy and use. It enables the implementation of essential use cases such as user and machine authentication on your information system, as well as ensuring the confidentiality of exchanged information. IDnomic PKI is enhanced by other products such as the Credential Management System (CMS) and Cryptovision solutions, enabling secure management and use of digital identities on cryptographic secure elements.





IDWAY, SOLUTIONS TO MANAGE YOUR POPULATION'S IDENTITY









IDway is a comprehensive suite of independent and interoperable modules for identity management. IDway manages the entire lifecycle of an individual's identity: from enrollment to the issuance of a unique legal identity. This identity, physical or digital, is based on multibiometric (face, fingerprints and iris). All components of IDway communicate with each other to create a strong, unified system. The components have standardized interfaces, making them easy to integrate into existing identity systems. Security and privacy are essential and are guaranteed at every step of the identity management

WORLDLINE WORLDLINE



WORLDLINE **DIGITAL IDENTITY**









A complete digital identity solution for a better user experience from enrollment to authentication, including lifecycle management and the application of trust services such as signature and electronic archiving. With eIDAS 2.0, Worldline completes its suite with Worldline Digital Identity Hub with a One-Stop Shop to simplify the acceptance of future digital identity wallets and enable digital identity-based transactions (payment, subscription, age control...) in One-Click.

Compliance: eIDAS, PSD2, and GDPR. Sectors: public institutions, banking, payment, healthcare, transport, retail.

IN GROUPE











Issuing, managing and automating PKI electronic certificates for people, services and objects to guarantee strong authentication, data confidentiality, integrity and electronic signatures with Nexus Certificate Manager PKI. Internationally recognized for almost 40 years by PKI experts.



















IN ORCHESTRATOR

IN Groupe is your partner in setting up a trusted infrastructure for the creation, storage and management of digital identities. This solution authenticates users and provides authentication services to third-party service providers (applications, websites or other digital services). It offers a wide range of functions: management of the lifecycle of the digital identity and its certificates (PKI), encryption of sensitive data (HSM) and eIDAS V2 electronic signature, and consent management. IN ORCHESTRATOR ensures long-term, consistent and secure management of the digital identity database at all times, according to the events transmitted to it.

43 Capacity offers Digital identity Capacity approach

















IDENTITY AND DIGITAL TRUST CONSULTING AND SUPPORT

The «Identity and Digital Trust Consulting and Support» offering by Blooo guides you through successful digital transformation based on tailored solutions that comply with upcoming standards. Leveraging our expertise in strategic positioning and comprehensive understanding of the European trusted digital ecosystem, we assist you in securely managing digital identity, protecting data, and establishing reliable trust mechanisms. Together, we build a robust digital environment ensuring confidentiality, integrity, and authenticity of information. Trust our experienced team to secure your digital future and achieve your strategic goals.

WORLDLINE WORLDLINE



WORLDLINE **DIGITAL IDENTITY**







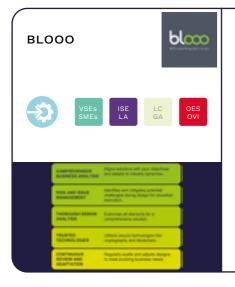




A complete digital identity solution for a better user experience from enrollment to authentication, including lifecycle management and the application of trust services such as signature and electronic archiving. With eIDAS 2.0, Worldline completes its suite with Worldline Digital Identity Hub with a One-Stop Shop to simplify the acceptance of future digital identity wallets and enable digital identity-based transactions (payment, subscription, age control...) in One-Click.

Compliance: eIDAS, PSD2, and GDPR. Sectors: public institutions, banking, payment, healthcare, transport, retail.





IDENTITY AND DIGITAL TRUST CONSULTING AND SUPPORT

The «Identity and Digital Trust Consulting and Support» offering by Blooo guides you through successful digital transformation based on tailored solutions that comply with upcoming standards. Leveraging our expertise in strategic positioning and comprehensive understanding of the European trusted digital ecosystem, we assist you in securely managing digital identity, protecting data, and establishing reliable trust mechanisms. Together, we build a robust digital environment ensuring confidentiality, integrity, and authenticity of information. Trust our experienced team to secure your digital future and achieve your strategic goals.

Capacity offers
Digital identity
Capacity approach





IDENTITY AND DIGITAL TRUST CONSULTING AND SUPPORT

The «Identity and Digital Trust Consulting and Support» offering by Blooo guides you through successful digital transformation based on tailored solutions that comply with upcoming standards. Leveraging our expertise in strategic positioning and comprehensive understanding of the European trusted digital ecosystem, we assist you in securely managing digital identity, protecting data, and establishing reliable trust mechanisms. Together, we build a robust digital environment ensuring confidentiality, integrity, and authenticity of information. Trust our experienced team to secure your digital future and achieve your strategic goals.



IDWAY, SOLUTIONS TO MANAGE YOUR POPULATION'S IDENTITY

IDway is a comprehensive suite of independent and interoperable modules for identity management. IDway manages the entire lifecycle of an individual's identity: from enrollment to the issuance of a unique legal identity. This identity, physical or digital, is based on multibiometric (face, fingerprints and iris). All components of IDway communicate with each other to create a strong, unified system. The components have standardized interfaces, making them easy to integrate into existing identity systems. Security and privacy are essential and are guaranteed at every step of the identity management process.





IDENTITY AND DIGITAL TRUST CONSULTING AND SUPPORT

The «Identity and Digital Trust Consulting and Support» offering by Blooo guides you through successful digital transformation based on tailored solutions that comply with upcoming standards. Leveraging our expertise in strategic positioning and comprehensive understanding of the European trusted digital ecosystem, we assist you in securely managing digital identity, protecting data, and establishing reliable trust mechanisms. Together, we build a robust digital environment ensuring confidentiality, integrity, and authenticity of information. Trust our experienced team to secure your digital future and achieve your strategic goals.



IDWAY, SOLUTIONS TO MANAGE YOUR POPULATION'S IDENTITY

IDway is a comprehensive suite of independent and interoperable modules for identity management. IDway manages the entire lifecycle of an individual's identity: from enrollment to the issuance of a unique legal identity. This identity, physical or digital, is based on multibiometric (face, fingerprints and iris). All components of IDway communicate with each other to create a strong, unified system. The components have standardized interfaces, making them easy to integrate into existing identity systems. Security and privacy are essential and are guaranteed at every step of the identity management process.

Capacity offers Digital identity Capacity approach



WORLDLINE **DIGITAL IDENTITY**









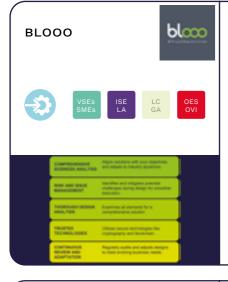




enrollment to authentication, including lifecycle management and the application of trust services such as signature and electronic archiving. With eIDAS 2.0, Worldline completes its suite with Worldline Digital Identity Hub with a One-Stop Shop to simplify the acceptance of future digital identity wallets and enable digital identity-based transactions (payment, subscription, age control...) in One-Click.

Compliance: eIDAS, PSD2, and GDPR. Sectors: public institutions, banking, payment, healthcare, transport, retail.





IDENTITY AND DIGITAL TRUST CONSULTING AND SUPPORT

The «Identity and Digital Trust Consulting and Support» offering by Blooo guides you through successful digital transformation based on tailored solutions that comply with upcoming standards. Leveraging our expertise in strategic positioning and comprehensive understanding of the European trusted digital ecosystem, we assist you in securely managing digital identity, protecting data, and establishing reliable trust mechanisms. Together, we build a robust digital environment ensuring confidentiality, integrity, and authenticity of information. Trust our experienced team to secure your digital future and achieve your strategic goals.



WORLDLINE **DIGITAL IDENTITY**



A complete digital identity solution for a better user experience from enrollment to authentication, including lifecycle management and the application of trust services such as signature and electronic archiving. With eIDAS 2.0, Worldline completes its suite with Worldline Digital Identity Hub with a One-Stop Shop to simplify the acceptance of future digital identity wallets and enable digital identity-based transactions (payment, subscription, age control...) in One-Click.

Compliance: eIDAS, PSD2, and GDPR. Sectors: public institutions, banking, payment, healthcare, transport, retail.

Capacity offers Digital identity Capacity approach

















IN Groupe is your partner in setting up a trusted infrastructure for the creation, storage and management of digital identities. This solution authenticates users and provides authentication services to third-party service providers (applications, websites or other digital services). It offers a wide range of functions: management of the lifecycle of the digital identity and its certificates (PKI), encryption of sensitive data (HSM) and eIDAS V2 electronic signature, and consent management. IN ORCHESTRATOR ensures long-term, consistent

and secure management of the digital identity database at all times,

according to the events transmitted to it.



TRUSTED SERVICES



EIDAS TRUST SERVICE PROVIDERS OF ELECTRONIC ATTESTATIONS ((Q)EAA), PROVIDER OF QUALIFIED CERTIFICATES AND VALIDATION OF QUALIFIED **CERTIFICATES**

CERTIGNA











Identify, Verify, Sign and Archive are the keys to the success of an electronic signature in a digital subscription process. Immediately available, easy to deploy and simple to use Certigna SIGN meets the majority of electronic signature requirements, whatever your sector of activity or business.

















Certigna provides a complete catalog of digital certificates for strong authentication, document signing and information encryption. Certigna certificates are elDAS, RGS, RGS**, RGS** / elDAS, 2D DOC qualified. The company also delivers qualified time-stamping and sovereign trust hosting services.

0

CERTIGNA TRUSTED SERVICES



51 **Capacity offers** Digital identity Capacity approach













Electronic certificates









for natural or legal persons

ChamberSign provide digital certificates for people and / or companies and they comply with the various RGS, eIDAS and ETSI regulations. They are in software format or on cryptographic supports. Digital IDs are used for strong authentication. They are also used for electronic signatures. It authenticates the signatory and guarantees his commitment and the integrity of the document. Stamp-type legal person certificates can certify the origin of the data, their integrity by the sealing mechanism. Some of them ensure the ownership of machines, servers, or domain names. Our products have been developed and designed in France since 2000.

IN GROUPE

000



NEXUS GO WORKFORCE













Trusted identities are fundamental to modern business. These identities enable you to digitize your company in complete security, and enable use cases such as multi-factor authentication, electronic signature (eIDAS-compliant), password-free log-in to Windows and SSO authentication. This solution also enables you to secure access to your physical resources (premises, parking lots, canteens, shared printers with Follow-me printing).



DIGITAL ARCHIVING AS DEFINED BY EIDAS



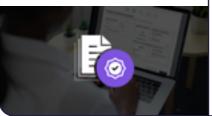












ARCHIPELS CERTIFY - CERTIFY AND VERIFY ANY DOCUMENT OR DATA INSTANTLY

Archipels Certify is an all-in-one SaaS solution for the certification and verification of data. It utilizes a sovereign blockchain infrastructure and provides guaranteed service level agreements (SLAs) to businesses. Bring trust to your data by securing it with blockchain technology, seamlessly integrating it into your business processes, and ensuring its verifiability and compliance with current regulations.

CERTIGNA











CERTIGNA SIGN

electronic signature in a digital subscription process. Immediately majority of electronic signature requirements, whatever your sector of activity or business.





53

ELECTRONIC SIGNATURE AND VERIFICATION

CERTIGNA



CERTIGNA SIGN









Identify, Verify, Sign and Archive are the keys to the success of an electronic signature in a digital subscription process. Immediately available, easy to deploy and simple to use Certigna SIGN meets the majority of electronic signature requirements, whatever your sector of activity or business.

















Certigna provides a complete catalog of digital certificates for strong authentication, document signing and information encryption. Certigna certificates are elDAS, RGS, RGS**, RGS** / elDAS, 2D DOC qualified. The company also delivers qualified time-stamping and sovereign trust hosting services.





ELECTRONIC SIGNATURE AND VERIFICATION

EVIDEN

















As organizations move to paperless transactions, it is necessary to electronically sign documents to guarantee their integrity and provide proof of acceptance by the signatory. The signature must undergo strict verification to detect any possible cause of invalidity. With IDnomic Sign, Eviden offers a global solution in the form of a platform for creating and verifying electronic signatures for different use cases, in compliance with European Directive 1999/93/EC and the eIDAS regulation. IDnomic Sign is available in Software-as-a-Service mode or installed on the customer's site.

ADVANCED TRACK & TRACE













SEALCRYPT



SEALCrypt® is a stand-alone data container for storing large quantities of encrypted information.

With its exceptional compactness and greater storage capacity than Datamatrix or QR-Code, it can contain text, photos, data and biometrics. It can be used to secure all types of documents, whether physical or digital.

The data is signed using asymmetric keys, guaranteeing the origin and integrity of the document content. Offline verification without connection is also possible. SEALCrypt code is 100% compliant with the EU's GDPR; the private data of the user are only entered in the code and remain under their sole control (in accordance with ISO 22385:2023, ISO 22376:2023, XP CEV Z42-105 and, if necessary, with AFNOR XP Z42-105).

55 Capacity offers Digital identity Capacity approach

ADVANCED TRACK & TRACE















VISIBLE DIGITAL SEAL / **SEALVECTOR**

SEALCrypt®/SEALVector® is a solution compatible with ISO 22376:2023 «Specification and usage of visible digital seal (VDS) data format for authentication, verification and acquisition of data carried by a document or object» and ISO 22385:2023 «Guidelines to establish a framework for trust and interoperability».

SEALCrypt®/SEALVector® is a physical media authentication solution, as defined in ISO 22381:2018, which can be operated using a simple

The physical dimensions of SEALCrypt $\mbox{\ensuremath{\$}/SEALVector}\mbox{\ensuremath{\$}}$ respecting the area allocated to 2D codes by the ICAO 9303 standard.

ARCHIPELS

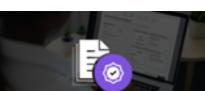












ARCHIPELS CERTIFY - CERTIFY AND VERIFY ANY DOCUMENT OR DATA INSTANTLY

Archipels Certify is an all-in-one SaaS solution for the certification and verification of data. It utilizes a sovereign blockchain infrastructure and provides guaranteed service level agreements (SLAs) to businesses. Bring trust to your data by securing it with blockchain technology, seamlessly integrating it into your business processes, and ensuring its verifiability and compliance with current regulations.











CERTIGNA SIGN

Identify, Verify, Sign and Archive are the keys to the success of an electronic signature in a digital subscription process. Immediately available, easy to deploy and simple to use Certigna SIGN meets the majority of electronic signature requirements, whatever your sector of activity or business.

ADVANCED TRACK & TRACE













SEALCRYPT



SEALCrypt® is a stand-alone data container for storing large quantities of encrypted information.

With its exceptional compactness and greater storage capacity than Datamatrix or QR-Code, it can contain text, photos, data and biometrics. It can be used to secure all types of documents, whether physical or digital.

The data is signed using asymmetric keys, guaranteeing the origin and integrity of the document content. Offline verification without connection is also possible. SEALCrypt code is 100% compliant with the EU's GDPR; the private data of the user are only entered in the code and remain under their sole control (in accordance with ISO 22385:2023, ISO 22376:2023, XP CEV Z42-105 and, if necessary, with AFNOR XP Z42-105).

57 Capacity offers Digital identity Capacity approach

ADVANCED TRACK & TRACE















VISIBLE DIGITAL SEAL / **SEALVECTOR**

SEALCrypt®/SEALVector® is a solution compatible with ISO 22376:2023 «Specification and usage of visible digital seal (VDS) data format for authentication, verification and acquisition of data carried by a document or object» and ISO 22385:2023 «Guidelines to establish a framework for trust and interoperability».

SEALCrypt®/SEALVector® is a physical media authentication solution, as defined in ISO 22381:2018, which can be operated using a simple smartphone.

The physical dimensions of SEALCrypt $\mbox{\ensuremath{\$}/SEALVector}\mbox{\ensuremath{\$}}$ respecting the area allocated to 2D codes by the ICAO 9303 standard.

ARCHIPELS

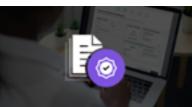












ARCHIPELS CERTIFY - CERTIFY AND VERIFY ANY DOCUMENT OR DATA INSTANTLY

Archipels Certify is an all-in-one SaaS solution for the certification and verification of data. It utilizes a sovereign blockchain infrastructure and provides guaranteed service level agreements (SLAs) to businesses. Bring trust to your data by securing it with blockchain technology, seamlessly integrating it into your business processes, and ensuring its verifiability and compliance with current regulations.

PERSONAL DEVICES



PERSONAL DEVICES AS DEFINED BY EIDAS

A3BC















TrustMe is a digital identity solution for private and public usage, compliant with the GDPR and eIDAS substantial level requirements. TrustMe allows end-users to create and manage their digital identity, to use strong authentication methods such as biometrics and to $\ensuremath{\mathsf{own}}$ an Id wallet to store their credentials and verify their authenticity. The end-user has total control over his data and is the only one who can give his consent to share all or part of his credentials. TrustMe relies on a patented storage protocol that protects data even in case of leakage and on market integration standards such as Open Id Connect and QR Code.

DOCAPOSTE

















The Digital Identity by The French Post is the first electronic identification means (2FA application) in France who have the requirements of the European eIDAS regulation for the substantial guaranteed level. It is based on the unique combination of an identifier, a mobile application, and a secret code. Available from FranceConnect and FranceConnect+ or in live, by this Digital Identity, you can make it possible to identify and authenticate natural persons in an immediate and recurring way to streamline and secure online

IDAKTO



IDCLUSTER



59





We offer the solution to go from physical identity to reusable digital identity. We help states to build a solid foundation for trust, enabling digital transformation. IDCluster provides a platform (Public or Private Cloud) and citizen applications on mobile devices, ensuring complete, transparent orchestration of the digital identity lifecycle. (KYC, SSO, MFA, CIAM, Wallet) With IDCluster, governments (e.g. Morocco and France) can offer a Secure, Reliable, and Inclusive Digital Identity, protecting personal data of their citizens. Service providers can identify and authenticate their users with assurance and without

IDEMIA



NATIONAL ID DOCUMENTS











IDEMIA offers fraud-resistant electronic national ID cards. The cards are made on a polycarbonate substrate, and integrate highend security features including LASINK™ color portraits and ID-One Cosmo X, a Common Criteria certified Java Card OS. Cosmo X can host multiple applications to fulfill eGovernment uses such as ICAO, eServices, QSCD, health cards, driver's licenses, etc. The security of Cosmo X and the applets integrated into the chip is guaranteed throughout the document's lifetime, thanks to JPatch. This advanced technology enables the remote updatability of the OS anytime,

IDEMIA













IDEMIA Smart Card Connector (ISCC) is a software component that links the physical ID card to digital services. It offers the eID card holder a secure authentication solution to access online services using the data stored in the chip. ISCC is based on the principles of multi-factor authentication: possession (the card), knowledge (the PIN) and inherence (fingerprints or face). It offers great flexibility of use as it enables access to eServices via a PC or a smartphone. This solution is based on the OpenID Connect protocol and can be integrated into any type of identity access management system.



PERSONAL DEVICES AS DEFINED BY EIDAS

IDEMIA



MOBILE ID









Mobile ID is a form of a digital identity that allows users to create and store their identity in the wallet app of their smartphone. The authenticity of the ID attributes is verified against an official system of record. Mobile ID is valid proof of identity for both in-person and online usage. Secure access to eServices is based on strong multifactor authentication: what the user owns (smartphone), what the user knows (PIN) and what the user is (biometrics). With Mobile ID, individuals have complete control over their personal data. During an identity check, they can choose to share specific personal information needed for the transaction.

NEOWAVE NEOWAVE













ID 2.0 RANGE

NEOWAVE's ID 2.0 Range is dedicated to protecting access to computer and mobile data. The products in this range come in the form of USB tokens (Weneo-A ID 2.0 and Winkeo-A ID 2.0) and smart cards (Badgeo ID 2.0) accompanied by their middleware (AET SafeSign IC). All these solutions integrate the same card component and its JavaCard OS certified Common Criteria EAL6+. Furthermore, they are manufactured in France. They are compatible with most business software applications (PKI, Logon, VPN, SSO, Encryption, electronic signature, etc.) and with various hardware equipment (physical access control, time management, etc.).

61 **Capacity offers** Digital identity Capacity approach



SYSTANCIA ACCESS



















Systancia Access is an access management (AM), user authentication (UA) and unique authentication (SSO) product. It provides a secure and centralized management of credentials as well as enhances user authentication through Multi-Factor Authentication (MFA). It provides users with a seamless access experience and offers auditing and reporting features to meet legal and regulatory obligations, depending on the industry. Systancia Access also drives performance and efficiency to the management of authentication resources, with solutions for application enrolment, enrolment of authentication devices (cards, keys, etc.), and a self-service portal for users who can unlock themselves, reducing the need to contact the organization's help desk.

THALÈS



SECURE IDENTITY DOCUMENTS





-0





As the leader on the market for ID documents - passports, ID cards, driving licenses, and health cards, Thales has extensive experience in secure physical ID schemes. The solutions provided are compliant with the highest levels of eIDAS security to allow and protect online access to services. Furthermore, secure documents from Thales have the highest level of electronic security thanks to their embedded software for ePassports and other electronic identity documents, which further reinforces the security of the document itself. Thales has a wide variety of innovative security systems at its disposal. These systems are fully customizable to meet needs.



AUTHENTIFICATION MEANS AND FACTORS

DOCAPOSTE







Digital identity

Capacity approach

VSE









The Digital Identity by The French Post is the first electronic identification means (2FA application) in France who have the requirements of the European eIDAS regulation for the substantial guaranteed level. It is based on the unique combination of an identifier, a mobile application, and a secret code. Available from FranceConnect and FranceConnect+ or in live, by this Digital Identity, you can make it possible to identify and authenticate natural persons in an immediate and recurring way to streamline and secure online journeys.

IDEMIA













IDEMIA offers fraud-resistant electronic national ID cards. The cards are made on a polycarbonate substrate, and integrate highend security features including LASINK™ color portraits and ID-One Cosmo X, a Common Criteria certified Java Card OS. Cosmo X can host multiple applications to fulfill eGovernment uses such as ICAO, eServices, QSCD, health cards, driver's licenses, etc. The security of Cosmo X and the applets integrated into the chip is guaranteed throughout the document's lifetime, thanks to JPatch. This advanced technology enables the remote updatability of the OS anytime, anywhere.





MOBILE ID

Capacity offers









Mobile ID is a form of a digital identity that allows users to create and store their identity in the wallet app of their smartphone. The authenticity of the ID attributes is verified against an official system of record. Mobile ID is valid proof of identity for both in-person and online usage. Secure access to eServices is based on strong multifactor authentication: what the user owns (smartphone), what the user knows (PIN) and what the user is (biometrics). With Mobile ID, individuals have complete control over their personal data. During an identity check, they can choose to share specific personal information needed for the transaction.

IDEMIA



IDEMIA SMART CARD CONNECTOR (ISCC)









IDEMIA Smart Card Connector (ISCC) is a software component that links the physical ID card to digital services. It offers the eID card holder a secure authentication solution to access online services using the data stored in the chip. ISCC is based on the principles of multi-factor authentication: possession (the card), knowledge (the PIN) and inherence (fingerprints or face). It offers great flexibility of use as it enables access to eServices via a PC or a smartphone. This solution is based on the OpenID Connect protocol and can be integrated into any type of identity access management system.

NEOWAVE



FIDO2 RANGE

















NEOWAVE offers FIDO2 products (USB security keys and smart cards) for strong authentication on the web and the cloud. Main characteristics: • 100% made in France • Based on secure components certified Common Criteria EAL5+ • Certified by ANSSI • Labeled «Cybersecurity Made in Europe» • Compliant with European security requirements • Compliant with FIDO2 ("Passwordless" authentication) and FIDO U2F (second factor authentication) specifications • Easy to install • Compatible with Azure Active Directory, Windows 10/11 and many web services (Gmail, Salesforce, Dropbox...) • Effective against phishing-type cyberattacks NEOWAVE is also referenced by Microsoft for its Passwordless solutions.



AUTHENTIFICATION MEANS AND FACTORS



SYSTANCIA ACCESS

ID 2.0 RANGE

control, time management, etc.).



Digital identity

Capacity approach

Systancia Access is an access management (AM), user authentication (UA) and unique authentication (SSO) product. It provides a secure and centralized management of credentials as well as enhances user authentication through Multi-Factor Authentication (MFA). It provides users with a seamless access experience and offers auditing and reporting features to meet legal and regulatory obligations, depending on the industry. Systancia Access also drives performance and efficiency to the management of authentication resources, with solutions for application enrolment, enrolment of authentication devices (cards, keys, etc.), and a self-service portal for users who can unlock themselves, reducing the need to contact the organization's help desk.

NEOWAVE

NEOWAVE

NEOWAVE's ID 2.0 Range is dedicated to protecting access to computer and mobile data. The products in this range come in the form of USB tokens (Weneo-A ID 2.0 and Winkeo-A ID 2.0) and smart cards (Badgeo ID 2.0) accompanied by their middleware (AET SafeSign IC). All these solutions integrate the same card component and its JavaCard OS certified Common Criteria EAL6+. Furthermore, they are manufactured in France. They are compatible with most business software applications (PKI, Logon, VPN, SSO, Encryption, electronic signature, etc.) and with various hardware equipment (physical access

SYSTANCIA



Capacity offers











NEOMIA PULSE

Neomia Pulse, an IC-MFA solution (Identity Control & MultiFactor Authentication) based on behavioral biometrics and contextual analysis, powered by Artificial Intelligence. Pulse seamlessly and without friction authenticates and controls any user by verifying their biometric identity. A strong authentication solution to secure any connection, whether in continuous mode (throughout an open session), or targeted (precise action at a given moment) and so prevent the malicious use of compromised accounts. Pulse meets the challenges of universality, user adoption, ease of deployment and cost, as no third-party system is required.

THALÈS



SECURE IDENTITY DOCUMENTS









As the leader on the market for ID documents - passports, ID cards, driving licenses, and health cards, Thales has extensive experience in secure physical ID schemes. The solutions provided are compliant with the highest levels of eIDAS security to allow and protect online access to services. Furthermore, secure documents from Thales have the highest level of electronic security thanks to their embedded software for ePassports and other electronic identity documents, which further reinforces the security of the document itself. Thales has a wide variety of innovative security systems at its disposal. These systems are fully customizable to meet needs.

SHAREID













ShareID offers various trusted digital SaaS services:

1. Doc IDV: Enables the verification of the authenticity of ID documents from more than 120 countries, with a precision level of up to 99.9%. 2. Full IDV: Integrates the Doc IDV service and enhances it by verifying the user's liveliness and document ownership. This service is available with or without operators.

3. MFA 3.0 (Multi-Factor Authentication): Strong authentication tied to government-issued IDs. It integrates the Full IDV service to issue a reusable digital identity without storing the users' personal or biometric data. Future interactions only require a simple smile to replicate the equivalent of a real-time identity check.



















IDEMIA offers fraud-resistant electronic national ID cards. The cards are made on a polycarbonate substrate, and integrate highend security features including LASINK™ color portraits and ID-One Cosmo X, a Common Criteria certified Java Card OS. Cosmo X can host multiple applications to fulfill eGovernment uses such as ICAO, eServices, QSCD, health cards, driver's licenses, etc. The security of Cosmo X and the applets integrated into the chip is guaranteed throughout the document's lifetime, thanks to JPatch. This advanced technology enables the remote updatability of the OS anytime,













IDEMIA SMART CARD CONNECTOR (ISCC)

IDEMIA Smart Card Connector (ISCC) is a software component that links the physical ID card to digital services. It offers the eID card holder a secure authentication solution to access online services using the data stored in the chip. ISCC is based on the principles of multi-factor authentication: possession (the card), knowledge (the PIN) and inherence (fingerprints or face). It offers great flexibility of use as it enables access to eServices via a PC or a smartphone. This solution is based on the OpenID Connect protocol and can be integrated into any type of identity access management system.

Capacity offers Digital identity Capacity approach



NEOMIA PULSE

Neomia Pulse, an IC-MFA solution (Identity Control & MultiFactor Authentication) based on behavioral biometrics and contextual analysis, powered by Artificial Intelligence. Pulse seamlessly and without friction authenticates and controls any user by verifying their biometric identity. A strong authentication solution to secure any connection, whether in continuous mode (throughout an open session), or targeted (precise action at a given moment) and so prevent the malicious use of compromised accounts. Pulse meets the challenges of universality, user adoption, ease of deployment and cost, as no third-party system is required.















IDEMIA offers fraud-resistant electronic national ID cards. The cards are made on a polycarbonate substrate, and integrate highend security features including LASINK™ color portraits and ID-One Cosmo X, a Common Criteria certified Java Card OS. Cosmo X can host multiple applications to fulfill eGovernment uses such as ICAO, eServices, QSCD, health cards, driver's licenses, etc. The security of Cosmo X and the applets integrated into the chip is guaranteed throughout the document's lifetime, thanks to JPatch. This advanced technology enables the remote updatability of the OS anytime,

NEOWAVE

NEOWAVE













ID 2.0 RANGE

NEOWAVE's ID 2.0 Range is dedicated to protecting access to computer and mobile data. The products in this range come in the form of USB tokens (Weneo-A ID 2.0 and Winkeo-A ID 2.0) and smart cards (Badgeo ID 2.0) accompanied by their middleware (AET SafeSign IC). All these solutions integrate the same card component and its JavaCard OS certified Common Criteria EAL6+. Furthermore, they are manufactured in France. They are compatible with most business software applications (PKI, Logon, VPN, SSO, Encryption, electronic signature, etc.) and with various hardware equipment (physical access control, time management, etc.).

69 Capacity offers

THALÈS



SECURE IDENTITY DOCUMENTS



Digital identity

Capacity approach







As the leader on the market for ID documents - passports, ID cards, driving licenses, and health cards, Thales has extensive experience in secure physical ID schemes. The solutions provided are compliant with the highest levels of eIDAS security to allow and protect online access to services. Furthermore, secure documents from Thales have the highest level of electronic security thanks to their embedded software for ePassports and other electronic identity documents, which further reinforces the security of the document itself. Thales has a wide variety of innovative security systems at its disposal. These systems are fully customizable to meet needs.

IN GROUPE



MULTI-APPLICATION IDENTITY CARDS











Use cases requiring face-to-face or remote identification, authentication or a qualified electronic signature. A digital identity can also be derived on a cell phone (IN Wallet). Ensuring the highest levels of security for personalized data stored on a chip or in a BioQR. Guaranteed authenticity and non-repudiation of the document. Based on IAS ECC technology, the various uses offered comply with the highest eIDAS levels.

71















THIQA, A CONSULTING OFFER

Since 2018, a team of experts specialized in digital trust Thiqa supports its clients in the selection, integration, development, implementation or operation of trusted services and solutions, in on-premises or Cloud mode. Thiqa has also an expertise in a portfolio of digital trust technologies including: PKI / CMS, Crypto / HSM boxes, Signature / validation / timestamping solutions, Strong authentication / IAM -CIAM, CLOUD Security...



Capacity offers

EVIDEN



EVIDEN CYBERSERVICES















Eviden supports companies and public authorities in their efforts to protect business-critical information and systems. We cover auditing, consulting, training, integration, managed services, and cybersecurity operations. We bring together proven expertise in the fields of Security Operation Center (SOC), Computer Security Incident Response & Tracking (CSIRT), Identity Management (IAM), Architects & DevSecOps, and Cloud security. Several of these areas of expertise are ANSSI-qualified. Eviden has its own laboratory for evaluating connected objects (IoT). The monitoring and R&D produced by our teams give rise to publications and contributions to (inter-)national programs.

DOCAPOSTE







THIQA, A CONSULTING OFFER

Since 2018, a team of experts specialized in digital trust Thiqa supports its clients in the selection, integration, development, implementation or operation of trusted services and solutions, in on-premises or Cloud mode. Thiqa has also an expertise in a portfolio of digital trust technologies including: PKI / CMS, Crypto / HSM boxes, Signature / validation / timestamping solutions, Strong authentication / IAM -CIAM, CLOUD Security...

72 Capacity offers Digital identity
Capacity approach









CONSULTING, SERVICES AND EXPERTISE FOR DIGITAL ID



Sopra Steria is a European leader in consulting for trusted digital services. Our group comprises various BUs (Defense and Security, Government, Consulting group Sopra Steria next) and subsidiaries (Galitt) that have developed operational and functional expertise in digital identity (of an individual, a legal entity, an employee) to build highly secure UX paths that respect high security and privacy. We support our customers (in the public sector, public administrations, the financial sector and payments) with state-of-the-art technologies and in compliance with current and future regulations (eIDAS, AML, DSP2, GDPR, NIS2, AI, etc.).

73Capacity offers

Digital identity
Capacity approach



PROJECT OWNERSHIP, OPERATIONAL ASSISTANCE, PROJECT/PROGRAM MANAGEMENT...





EVIDEN CYBERSERVICES















Eviden supports companies and public authorities in their efforts to protect business-critical information and systems. We cover auditing, consulting, training, integration, managed services, and cybersecurity operations. We bring together proven expertise in the fields of Security Operation Center (SOC), Computer Security Incident Response & Tracking (CSIRT), Identity Management (IAM), Architects & DevSecOps, and Cloud security. Several of these areas of expertise are ANSSI-qualified. Eviden has its own laboratory for evaluating connected objects (IoT). The monitoring and R&D produced by our teams give rise to publications and contributions to (inter-)national programs.

IDEMIA







PUBLIC-PRIVATE & IDENTITY PARTNERSHIPS IN IDENTITY MANAGEMENT

IDEMIA has in-depth expertise in identity management and therefore accompanies governments in the implementation of large-scale projects such as the digitalization of ID documents. We provide a comprehensive offer, starting from the initial concept to implementation and support and maintenance. By selecting IDEMIA, you will benefit from: • Our experienced teams with excellent project management skills • Technical guidance: recommendations on electronic chips and OS, compliant with the latest standards, integration support, etc. • Innovations in physical, electronic and digital security features • Risk sharing (financial and operating) • Technology transfer (audit, product specification, training and maintenance and support).

Capacity offers

PROJECT OWNERSHIP, OPERATIONAL ASSISTANCE, PROJECT/PROGRAM MANAGEMENT...



CONSULTING, SERVICES AND EXPERTISE FOR DIGITAL ID







Sopra Steria is a European leader in consulting for trusted digital services. Our group comprises various BUs (Defense and Security, Government, Consulting group Sopra Steria next) and subsidiaries (Galitt) that have developed operational and functional expertise in digital identity (of an individual, a legal entity, an employee) to build highly secure UX paths that respect high security and privacy. We support our customers (in the public sector, public administrations, the financial sector and payments) with state-of-the-art technologies and in compliance with current and future regulations (eIDAS, AML, DSP2, GDPR, NIS2, AI, etc.).

Capacity offers

DIGITAL IDENTITY ADMINISTRATION



EVIDEN

















Evidian offers a complete range of identity and access management (IAM) solutions to improve security and productivity within organizations. Our core offerings cover the following products: • Evidian Analytics: data analysis and reporting • Evidian Authentication Manager: Multi-factor authentication • Evidian IDaaS: Identity as a Service • Evidian IGA: Identity Governance and Administration • Evidian Safekit: high-availability software for applications: • Evidian WAM: Web Access Manager • Enterprise SSO: Single Sign-On • Self-Service Password Reset (SSPR): Resetting Windows passwords.

Digital identity

Capacity approach

























SYSTANCIA IDENTITY



Systancia Identity is an identity governance and administration product (IGA). It provides a repository of workforce identities and enables to manage their authorizations, ensuring perfect consistency between your HR and production information system, automating your access request workflows, your workforce arrival, mobility or departure process, and automatically provisioning accounts and rights in target applications and systems. The product also enables you to guarantee the coherence of authorizations (SoD) and to manage rights certification campaigns. Based on a combination of ABAC and OrBAC models, it enables agile management of rights and authorizations in multi-identity/multi-organization contexts.



IN GROUPE



NEXUS SMART ID









Nexus SmartID provides solutions for managing and using physical and logical identities, as well as for connected devices and objects. This solution integrates PKI, CMS, SmartPhone applications, etc. to manage and use all your digital identities.



IDAKTO



IDCLUSTER









We offer the solution to go from physical identity to reusable digital identity. We help states to build a solid foundation for trust, enabling digital transformation. IDCluster provides a platform (Public or Private Cloud) and citizen applications on mobile devices, ensuring complete, transparent orchestration of the digital identity lifecycle. (KYC, SSO, MFA, CIAM, Wallet) With IDCluster, governments (e.g. Morocco and France) can offer a Secure, Reliable, and Inclusive Digital Identity, protecting personal data of their citizens. Service providers can identify and authenticate their users with assurance and without

78 Capacity offers Digital identity Capacity approach





















Evidian offers a complete range of identity and access management (IAM) solutions to improve security and productivity within organizations. Our core offerings cover the following products: • Evidian Analytics: data analysis and reporting • Evidian Authentication Manager: Multi-factor authentication • Evidian IDaaS: Identity as a Service • Evidian IGA: Identity Governance and Administration • Evidian Safekit: high-availability software for applications: • Evidian WAM: Web Access Manager • Enterprise SSO: Single Sign-On • Self-Service Password Reset (SSPR): Resetting Windows passwords.























SYSTANCIA IDENTITY



Systancia Identity is an identity governance and administration product (IGA). It provides a repository of workforce identities and enables to manage their authorizations, ensuring perfect consistency between your HR and production information system, automating your access request workflows, your workforce arrival, mobility or departure process, and automatically provisioning accounts and rights in target applications and systems. The product also enables you to guarantee the coherence of authorizations (SoD) and to manage rights certification campaigns. Based on a combination of ABAC and OrBAC models, it enables agile management of rights and authorizations in multi-identity/multi-organization contexts.

79 **Capacity offers** Digital identity Capacity approach



EVIDEN



EVIDIAN IAM











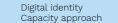
Evidian offers a complete range of identity and access management (IAM) solutions to improve security and productivity within organizations. Our core offerings cover the following products: • Evidian Analytics: data analysis and reporting • Evidian Authentication Manager: Multi-factor authentication • Evidian IDaaS: Identity as a Service • Evidian IGA: Identity Governance and Administration • Evidian Safekit: high-availability software for applications: • Evidian WAM: Web Access Manager • Enterprise SSO: Single Sign-On • Self-Service Password Reset (SSPR): Resetting Windows passwords.

80 **Capacity offers**

Digital identity Capacity approach



Capacity offers





TOOLS FOR DECENTRALIZED, DISTRIBUTED SSID ADMINISTRATION WITH OR WITHOUT DLT/ BLOCKCHAIN

ARCHIPELS













ARCHIPELS CONNECT - TRUST BY DESIGN WITH DECENTRALIZED IDENTITY FOR YOUR **CLIENTS AND PARTNERS**

Archipels Connect creates an ecosystem of extended identities through the creation of verifiable credentials to secure and simplify exchanges. With Archipels Connect, you can create and manage verifiable digital attestations for identity management, securing B2B and B2G exchanges, and simplifying the online user experience regarding authentication issues.

SHAREID















SHAREID

ShareID offers various trusted digital SaaS services:

1. Doc IDV: Enables the verification of the authenticity of ID documents from more than 120 countries, with a precision level of up to 99.9%. 2. Full IDV: Integrates the Doc IDV service and enhances it by verifying the user's liveliness and document ownership. This service is available with or without operators.

3. MFA 3.0 (Multi-Factor Authentication): Strong authentication tied to government-issued IDs. It integrates the Full IDV service to issue a reusable digital identity without storing the users' personal or biometric data. Future interactions only require a simple smile to replicate the equivalent of a real-time identity check.

SECURITY COMPONENTS













SECURE IDENTITY SOLUTIONS

At STMicroelectronics, the European leader in semiconductors, we provide a wide range of chips and solutions that meet requirements for both performance and security of numerous application domains, including electronic identity documents. The ST31, ST33, and ST54 secure microcontroller families are certified at the highest level for security. They enable the secure storage of an individual's sensitive information in identity cards and passports, and of digital identity on mobile platforms. We offer STeID software solutions to our clients and partners; the STeID family is a portfolio of turnkey identity solutions compatible and interoperable with market standards.



Capacity offers



SMART CARD READERS

The NEOWAVE range of smart card readers simplifies the implementation of multiple secure applications (payment, identity, loyalty, transportation, access control, network security, healthcare, and more). They are easily installed, deployed, and integrated into an office environment thanks to their PS/SC CCID compatibility. They are compatible with Windows, Linux, Mac and Android operating systems and do not require any driver installation. They come in the form of contact and/or contactless smart card readers (RFID/NFC) as well as Micro and Mini-SIM card reader USB keys.

85























With its data protection solutions, Eviden's Trustway product range guarantees the confidentiality of your sensitive data and protects you against the risks of cyber-attacks. European specialist in data encryption, Eviden offers a wide range of products including Security Hardware Modules (HSM) for general use with its Trustway Proteccio™, or for securing transactions with Trustway Crypt2pay. Eviden also guarantees the confidentiality of your data with its Trustway IP Protect network encryptor. Our products comply with the most stringent standards and certifications, enabling you to meet the most demanding requirements.



Capacity offers













SECURE IDENTITY SOLUTIONS

At STMicroelectronics, the European leader in semiconductors, we provide a wide range of chips and solutions that meet requirements for both performance and security of numerous application domains, including electronic identity documents. The ST31, ST33, and ST54 secure microcontroller families are certified at the highest level for security. They enable the secure storage of an individual's sensitive information in identity cards and passports, and of digital identity on mobile platforms. We offer STeID software solutions to our clients and partners; the STeID family is a portfolio of turnkey identity solutions compatible and interoperable with market standards.

86 Capacity offers

Digital identity Capacity approach 87



MOBILE DEVICE COMPONENTS FOR SECURE STORAGE OF KEYS OR CONTENT (TEE, WHITEBOX, VIRTUAL SIM, ...)











SECURE IDENTITY SOLUTIONS

At STMicroelectronics, the European leader in semiconductors, we provide a wide range of chips and solutions that meet requirements for both performance and security of numerous application domains, including electronic identity documents. The ST31, ST33, and ST54 secure microcontroller families are certified at the highest level for security. They enable the secure storage of an individual's sensitive information in identity cards and passports, and of digital identity on mobile platforms. We offer STeID software solutions to our clients and partners; the STeID family is a portfolio of turnkey identity solutions compatible and interoperable with market standards.

COMPANY INDEX



90 Company index Digital identity Capacity approach

A3BC



CONTACT

Houssem KHEMIRI +33673568342 houssem.khemiri@a3bc.io https://identitenumerique.trustmeid.io/fr/









SEGMENTS

Member of



A3BC - Anything, Anytime, Anywhere Biometric Connections. It is a French Tech private actor, whose purpose is to complete government by offering to all citizens a universal digital Id combined with Strong Customer Authentication methods. Our platform relies on biometric factors, independent from GAFAM, to secure personal data and simplify its use. Our data storage protocol is patented and fulfill the highest cyber-security market standards. Our platform is compliant with **GDPR European regulation**. We have successfully passed the first two milestones (J0/J1) of EU eIDAS certification (electronic IDentification, Authentication and trust Services) and are now executing towards the next milestones. Our company is already funded by the biggest EU Bank and supported by the French government. Our goal is the give to every citizen the full and exclusive control over its personal data. We provide trust between parties to guarantee individuals a secured access to any service. We want anyone to be able to fully manage its life in the digital world just as in the physical one!



91 Company index Digital identity Capacity approach

Advanced Track and Trace



CONTACT

Zbigniew SAGAN +33147166472 & +33607379687 z.sagan@att-fr.com https://www.att-fr.com







CRITERIA



SEGMENTS

Member of



Advanced Track & Trace (ATT) is a French company founded in 2003. ATT became a global leader and technology provider in brand protection, and document security providing confidence and trust. We develop innovative solutions – in authentication, identification, traceability, anti-counterfeiting and serialization – for a better protection of products, documents, organizations, and citizens.

ATT technologies have been applied to over 20 billion products/documents/bills over the past 10 years, notably for the Banque de France (banknotes), tax stamps for tobacco and alcohol, identity documents, but also in the cosmetics, wines and spirits, luxury goods and pharmaceuticals sectors."

ATT is a Founding Member of the Visible Digital Seal International Council (VDSIC - ISO 15459-compliant Issuing Agency) and has actively participated in the development of AFNOR XP Z42-105, ISO 22385 and ISO 22376 standards. Since 2023, a VDS compliant with these standards has ensured the protection of the France CyberSecurity labels that ATT has implemented as part of the Otentik Trusted Network.

92 Company index Digital identity Capacity approach

Archipels



CONTACT

hanane@archipels.io







Member of



Archipels is a decentralized identity platform to simplify data exchanges and to strengthen trust between organizations and individuals. Secure information sharing and make communication more efficient.

The future of Digital Identity

Certification - Verification - Identification

93 Company index Digital identity Capacity approach

Blooo



CONTACT

Mickaël GABORIT 0972377726 trust@blooo.io https://blooo.io/













SEGMENTS

Member of



Blooo is a major player in the consulting and development of digital trust solutions, with a strong emphasis on cybersecurity and compliance. Adhering to the rigorous standards of ISO27001 and the NIS 2 European Directive, our multidisciplinary team employs advanced penetration testing (pentesting) methodologies to ensure robust digital security. We leverage the benefits of distributed infrastructures, decentralized architectures (Blockchain), and identity or digital asset vaults, while ensuring the highest standards of security and data protection. These schemes not only allow companies to retain the benefits of digital platforms but also ensure industrial or personal sovereignty over data, in line with global cybersecurity standards. We offer in-depth case studies, customized solution scoping, implementation, and deployment of blockchain solutions. Whether you're a trusted enterprise, institution, or consortium, we're here to help you harness the benefits of decentralization, while ensuring robust cybersecurity measures, leading you confidently into a secure, sovereign digital future.



94 Company index Digital identity Capacity approach

Certigna



CONTACTS

Emmanuelle GENESTINE (Certigna SIGN / Certigna VERIF ID / Certigna DIGITAL ID) +33787835963

emanuelle.genestine@tessi.fr

Gaetan PACCOU (Services de confiance Certigna) +33607198706 gaetan.paccou@tessi.fr www.certigna.com







SEGMENTS

CRITERIA

Member of



As a trusted third party, Certigna guarantees the chain of trust needed to secure every stage of its customers' business processes, through a range of trusted products including a remote identity verification platform, a reusable digital identity service, an electronic signature platform and trusted services (RGS / eIDAS electronic certificates, qualified time stamping, encryption, electronic archiving, sovereign hosting).

95 Digital identity Company index Capacity approach

Chambersign



CONTACT

Guillaume PETIT 0892230252 commercial@chambersign.fr www.chambersign.fr























Member of



Chambersign is a Trust Service Provider created in 2000. Chambersign delivers professional digital identity tools for physical persons and legal entities. They are issued and delivered in compliance with the strictest industry standards, guaranteeing an optimum level of security for digital exchanges. The professional digital identities and electronic certificates for physical persons and legal entities are issued in compliance with the regulations (RGS and eIDAS). Multi-purpose, they enable strong authentication, electronic signatures, data sealing, traceability of data repositories and secure access and electronic exchanges.

Pioneers in their field, ChamberSign has always supported private and public organizations, small and medium-sized businesses and SMEs in securing their electronic exchanges and using electronic certificates and/or seals to best meet their needs.

ChamberSign received the ANSSI security visa for its electronic certification services and the France CyberSecurity Label. It is ISO 9001:2015 certified. Its processes and information system have undergone an RGPD compliance audit.

DIGITAL TRUST









96 Company index

Digital identity Capacity approach

Digital identity Company index Capacity approach

Docaposte



CONTACTS

Nicolas BIGAND (L'Identité Numérique La Poste) nicolas.bigand@laposte.fr

> Simon-Pierre de La Seigliere (ID360 / L'Identité Numérique La Poste) simon-pierre.delaseigliere@docaposte.fr

> > Gaëlle PICARD (Thiqa) gaelle.picard@docaposte.fr













Member of



A subsidiary of La Poste Group, Docaposte is the digital trust leader in France.

Docaposte supports all companies and public institutions with their transformation, enabling them to accelerate it with confidence.

Docaposte is a technology specialist that promotes the development of digital uses by businesses and citizens within an ethical and sovereign framework.

Docaposte has over 40,000 corporate and public sector customers, more than 7,500 employees at 86 sites in France and abroad, and sales of €826 million in 2022.

Its offer is one of the broadest on the market, combining both trusted digital and in-person services:

- expertise & consulting,
- tailor-made or ready-to-use trusted solutions,
- service excellence.

This makes it possible to cover every need for every organization.

Docaposte uses its expertise as an integrator to build BtoB and BtoC service platforms aimed at reconciling multiple environments to simplify and facilitate information exchanges and customer journeys, with the assurance of highly secure data.

As an expert in the processing of sensitive data, and France's leading operator of healthcare data (45 million medical records), Docaposte masters the entire transaction processing chain - identification, authentication, signature, certification, and archiving - benefiting from a unique positioning on the market that enables it to meet a customer's needs end-to-end, in compliance with regulations and with the assurance of highly secure data.

Eviden

97

EVIDEN

CONTACT

Dan BUTNARU +33682554509 dan.butnaru@atos.net https://www.eviden.com





















Eviden brings together the Digital, Cloud, Big Data and Security activities of Atos and will be an international leader in reliable, sustainable, data-driven digital transformation. As a key player in next-generation digital and a global leader in cloud, data, advanced computing and security, Eviden will bring its expertise to all business sectors, in more than 53 countries. The orchestration of cuttingedge technologies across the digital continuum, combined with the expertise of its 57,000 talents, will enable Eviden to extend the potential of solutions available to enterprises and public authorities, helping to shape their digital future. Within the Atos Group, Eviden's activities generate annual sales of around €5 billion. Our products and services provide key technological building blocks for French and European strategic autonomy.



98 Company index Digital identity Capacity approach

iD3 Technologies



CONTACT

Marc LAVOREL +33476757585 marc.lavorel@id3.eu https://bioseal.codes/













id3 Technologies, an independent company, innovates in the advanced techniques of Artificial Intelligence and computer vision. Thanks to the biometric and document recognition algorithms developed in our R&D department, our ambition is to ensure the authenticity and legitimacy of the billions of objects, goods and documents we create, use or consult every day, as well as the identity of their holder.

99 Company index

IDAKTO



CONTACT

Yann BOUAN +33185401270 contact@idakto.com https://www.idakto.fr/





CRITERIA





Digital identity Capacity approach









iDAKTO guarantees a high level of trust through its digital solutions. We offer leading-edge solutions by providing full integration of the digital identity lifecycle, from registration to online identity verification. With us, privacy is non-negotiable. Confidentiality is at the heart of our approach, applying international standards and the requirements of the General Data Protection Regulation. We guarantee inclusive, sovereign and secure transactions. Whether they are familiar with the digital world or not, all citizens have the right to easy access to private and public digital services. Secure interactions with personal data: our platform protects every user against identity theft and safeguards personal data from prying eyes throughout the digital journey.



100 Company index

101

Idemia



CONTACTS

Guillaume BERTEAU (IDway) guillaume.berteau@idemia.com

Thomas POREAUX (Documents d'identité / Partenariats publics privés dans la gestion de l'identité) thomas.poreaux@idemia.com

> Suzie BEGIN (Mobile ID) suzie.begin@idemia.com

Lauriane COUTURIER (ISCC) Lauriane.couturier@idemia.com

Catherine KIENLEN (Solutions d'enrôlements) Catherine.kienlen@idemia.com



Digital identity

Capacity approach



















Member of

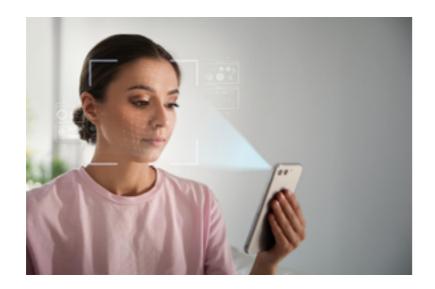


As leader in identity technologies, IDEMIA is on a mission to unlock the world and make it safer. Backed by cutting-edge R&D, IDEMIA provides unique technologies, underpinned by long-standing expertise in biometrics, cryptography, data analytics, systems and smart devices.

IDEMIA offers its public and private customers payment, connectivity, access control, travel, identity and public security solutions. Every day, around the world, IDEMIA secures billions of interactions in the physical and digital worlds.

With nearly 15,000 employees, IDEMIA is trusted by over 600 governmental organizations and more than 2,300 enterprises spread over 180 countries, with an impactful, ethical and socially responsible approach.

For more information, visit www.idemia.com and follow @IDEMIAGroup on Twitter.



IN Groupe



CONTACTS

Charles LAHOGUE (Nexus Certificate Manager (PKI) / Nexus GO Workforce / TAME 3 S / Nexus Smart ID) charles.lahogue@ingroupe.com https://ingroupe.com/fr/

Pascal JANER (IN Wallet / IN Orchestrator / Cartes d'identité multi-applicatives) pascal.janer@ingroupe.com https://ingroupe.com/fr/



























Member of



As global specialist in identity and secure digital services, IN Groupe is the trusted partner in the management and protection of sensitive data. By mastering the entire valuechain of the identity, IN Groupe has deployed its expertise beyond sovereign identity by extending its solutions and services to professional identities and identity of things. A stakeholder in major issues aimed at improving and securing the right to be yourself in the digital age, the Group regularly intervenes with institutions and organizations involved in the identity ecosystem in Europe. IN Groupe's solutions, at the cutting edge of technology, integrate electronic, optical, holographic and biometric technologies, at the service of States, businesses and citizens. The Group operates 4 reference brands, each a leader in their respective markets. IN Groupe for physical and digital identity solutions for Governments and administrations, Nexus for secure identity solutions for professionals and objects, SPS for electronic components and package solutions for banking and identity, Surys for optical and holographic components for the banknote and identity market as a national state printing company, IN Groupe is a committed player in the most protective and secure digital identity schemes.

IN GROUPE IN FIGURES (2022 turnover): €516m 1,900 employees - 10 sites in Europe - 8 sales offices around the world. + 130 countries using IN Groupe' solutions - 30 partner governments.

102 Company index Digital identity Capacity approach

Merox



CONTACT

Michael CARLETTO 0764212859 michael.carletto@merox.io https://www.merox.io/





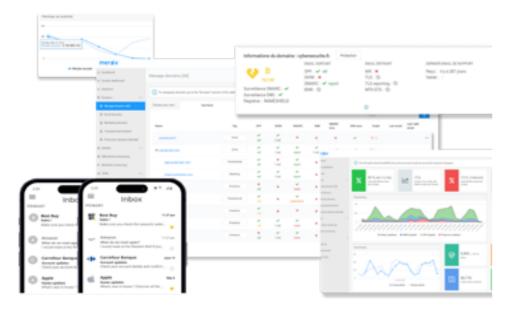




CRITERIA



"Merox is a European (France) software company established by a team of former consultants who are experts in cyber security and messaging systems. Its eponymous platform supports organizations in securing their DNS and domain names by offering an «all-in-one» SaaS solution. It offers complete mapping and control of the DNS environment, analysis of DMARC reports, monitoring and verification of DNS entries, monitoring of blacklists, tools to help implement security protocols, security alerts and monitoring of "lookalike" domains. With Merox, organizations can control their DNS environment, prevent identity theft, reduce phishing, protect their brand and increase email deliverability. The solution is recognized by Gartner as one of the 10 best solutions worldwide, and the only one in France. Merox is also active in the French and international ecosystem, as a member of numerous digital and cybersecurity associations. Customers ranging from the CAC40 to SMEs place their trust in Merox across a wide range of sectors, including banking, insurance, healthcare, government and industry."



103 Company index

Neowave

NEOWAVE

CONTACT

Bruno BERNARD 0624022045 bruno.bernard@neowave.fr https://neowave.fr/fr/produits/gamme-fido/











Digital identity

Capacity approach











Member of



NEOWAVE is a company specialized in strong authentication and secure transactions. Its mission is to protect the digital assets of companies and users through strong authentication technologies using secure components (Common Criteria EAL5+ certified) and digital certificates. Its solutions address the cybersecurity, digital trust and identity management markets. NEOWAVE offers three product families:

- ID 2.0 solutions (smart cards and USB keys) for strong authentication using certificates,
- The FIDO range (smart cards and FIDO-compatible USB keys) for strong authentication on the Web and in the cloud,
- USB or Bluetooth contact and/or contactless (RFID/NFC) smart card readers for the implementation of multiple secure applications in professional environments.

NEOWAVE's solutions meet the security needs of public authorities, operators of vital importance (OIV) and companies seeking effective protection for their sensitive data. They are entirely manufactured in France and comply with the security requirements of European agencies such as RGS, eIDAS, GDPR, PSD2 and NIS."



104 Company index Digital identity Capacity approach

Orange Business



Business

CONTACTS

securite/live-identity

Antoine MAISONNEUVE (Live Identity Wallet)
+33685304362
antoine.maisonneuve@orange.com
https://www.orange-business.com/fr/solutions/

Aziz HAOUAS (Live Identity Verify)
+33786000885
aziz.haouas@orange.com
https://www.orange-business.com/fr/solutions/
securite/live-identity











SEGMENTS

Member of



A key player in digital trust, Orange Business is an expert in the network, connectivity, data, cloud, identity management and cybersecurity. At Orange Business, digital trust is built on resilient infrastructure, tailored services and state-of-the-art cybersecurity products with the expertise of Orange Cyberdefense. Finally, digital trust translates into compliance with regulations and certifications. Our aim is to create a positive impact for our customers and for society as a whole, with a commitment to transparency and openness! That's why Orange Business' digital identity offerings are the foundation of trust that enables our customers to carry out transactions with their ecosystems with complete peace of mind, especially in European dataspaces, where hundreds of companies are interconnected to exchange data with complete confidence.



105 Company index Digital identity Capacity approach

ShareID



CONTACT

Sara SEBTI +33632987132 sara.sebti@shareid.ai https://shareid.ai















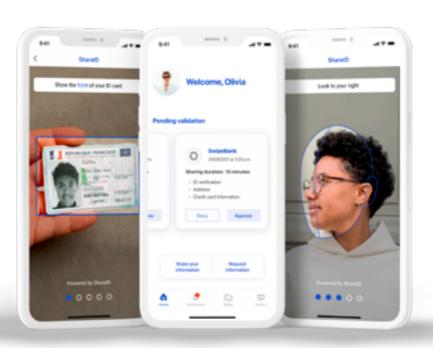






ShareID is an authentication-as-a-service (AaaS) solution tied to government-issued IDs. After an initial capture of the user's identity document and face, we issue a reusable digital identity, without storing personal or biometric data, enabling businesses to trigger on-demand an ID verification or verified personal data sharing in real-time, with a simple smile, and with a zero-trust/zero-knowledge proof. Some of our features:

- Liveness and anti-spoofing algorithms that can detect deep fakes and silicon masks...
- A precision rate of 99.9% on document authenticity covering 120+ countries thanks to our partnership with the French Military Police.
- Patented technology for digital identity issuance.
- Patented Biometric Chain Encryption for personal data security.
- We never store users' data or biometrics.
- We provide a frictionless user experience at each transaction that requires an ID check.
- Compliant with international laws for personal data protection and privacy.



106 Company index

Digital identity Capacity approach

107

Sopra Steria



CONTACTS

Jean-Luc GIBERNON (Conseil, Services et Expertise pour l'identité numérique) +33681278652 jean-luc.gibernon@soprasteria.com

> Youssef TALBAOUI (Capitole) +33610124861 youssef.talbaoui@soprasteria.com















SEGMENTS

Member of



Our mission is to provide trusted solutions and services to the most exposed public and private actors, to ensure the resilience of their critical systems and protect their sensitive information assets. In Europe, compliance with national regulations guarantees confidence and state of the art. Our teams support you throughout the security life cycle, from prevention to protection and detection-reaction. Our tailor-made approach adapts to your context and your technological and budgetary constraints, around a service model combining proximity and industrialization. At the core of the cybersecurity and crisis management domains, the quality and the proximity of the trust-based relationship with our customers are fundamental for us. Listening to your specific needs and the initiatives of our experts, we seek to improve constantly to provide you with effective and innovative solutions!"



STMicroelectronics



CONTACT

Eric BULTEL +33760492657 eric.bultel@st.com https://www.st.com/en/secure-mcus/banking-idtransport.html













SEGMENTS

Member of



At ST, we are more than 50,000 creators and makers of semiconductor technologies mastering the semiconductor supply chain with state-of-the-art manufacturing facilities. An integrated device manufacturer, we work with more than 200,000 customers and thousands of partners to design and build products, solutions, and ecosystems that address their challenges and opportunities, and the need to support a more sustainable world. Our technologies enable smarter mobility, more efficient power and energy management, and the wide-scale deployment of the Internet of Things and connectivity. We are committed to achieving our goal to become carbon neutral on scope 1 and 2 and partially scope 3 by 2027. By 2022, we are the European leader in the semiconductor market, with net sales of \$16.1 billion. Further information can be found at www.st.com.



108 Company index Digital identity Capacity approach

Systancia



CONTACTS

Valérie GIGOU (Systancia Identity / Systancia Access) commercial@systancia.com https://www.systancia.com/systancia-identity/

> Xavier HAMEROUX (Neomia Pulse) x.hameroux@neomia.ai

















SEGMENTS

Member of



Systancia is a global ISV (independent software vendor) securing workforces' access to their working environments.

Our vision is that "trust drives performance".

Our mission is to provide workforces with all the cyber elements they need to deliver business performance through cyber trust.

Therefore, we put together our own technologies into a single platform which delivers user productivity and organization efficiency thanks to a combination of speed and ease of use.

Systancia's Zero Trust platform provides workforces whatever their context (at the office, working from home, industrial operators, third parties'...) with a seamless and immediate access (business or privileged, local or remote, ...) to all resources they need to do their day-to-day work (cloud apps, applications in the organization datacenter, desktops, data, IT & OT systems, services, etc.).



Digital identity 109 Company index Capacity approach

Thalès THALES Building a future we can all trust

CONTACT

Béatrice ROYER 0442366666 beatrice.royer@thalesgroup.com https://www.thalesgroup.com/en/markets/ digital-identity-and-security





CRITERIA







Member of



Thales is a global technology leader with more than 77,000 employees on five continents. The Group is investing in digital and "deep tech" innovations - Big Data, artificial intelligence, connectivity, cybersecurity and quantum technology - to build a future we can all trust.

In the markets of defense and security, aerospace and space, digital identity and security, and transport, Thales provides solutions, services and products to help its customers - companies, organizations and governments - to carry out their critical missions.

Combining a unique diversity of expertise, talents and cultures, our architects design and deliver high technology solutions. Solutions that make tomorrow possible, today. Whenever a critical decision needs to be made, Thales has a role to play. Our solutions help customers to make the right decisions at the right time and act accordingly in challenging environments.



110 Company index

Digital identity Capacity approach

Company index

111

Digital identity Capacity approach

Worldline

WORLDLINE NWW.

CONTACT

Etienne PLOUVIER
0603989514
etienne.plouvier@worldline.com
https://worldline.com/en/home/mainnavigation/solutions/financial-institutions/
authentication-and-security/digital-identity.html











SEGMENTS

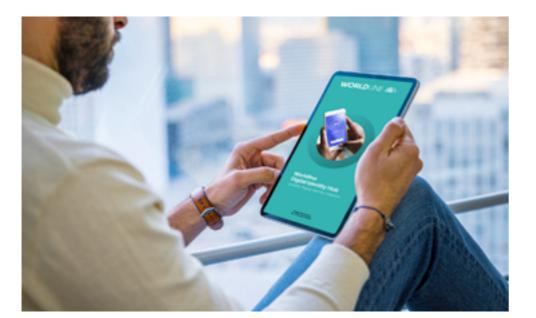
Member of



Our solutions ensure secure payments and trusted transactional services along the entire payments value chain, enabling sustainable economic growth.

Services offered by Worldline include instore and online commercial acquiring, highly secure payment transaction processing and numerous digital services. Our continuously growing portfolio of solutions is environmentally friendly and supports trust and social transformation.

Trust and sustainability are at the heart of everything we do. Our vision is to enable sustainable economic growth and reinforce trust and security in our societies. We do this by ensuring our trusted solutions are environmentally friendly, widely accessible and support social transformation.



112 About ACN Digital identity Capacity approach

ABOUT ACN

The Digital Trust Alliance (Alliance pour la Confiance and Europe. It has worked on all the major texts Numérique - ACN) represents organizations (world for our sector, such as the creation of the French leaders, SMEs, mid-sized enterprises, and micro- national electronic identity card (CNIe), for which enterprises) in the digital trust sector, particularly its members contributed with their technical those specialized in digital identity, cybersecurity, expertise. ACN also played a very active role in and trusted artificial intelligence. In this field, the construction of the European eIDAS regulation France boasts highly efficient industrial cooperation (2014), as well as in the various constituent stages and internationally recognized excellence thanks that, since 2011, have shaped the emergence of to world leaders, SMEs, mid-sized companies, and a national digital identity project, through the the various dynamic actors in the sector.

ACN brings together all the major groups and numerous ETIs, SMEs, VSEs and start-ups involved ACN is a member of the Federation of Electrical, concerning digital identity. It is currently heavily Industries. involved in European work on the revision of the eIDAS regulation creating a European wallet for ACN is also a founding member of the European digital identities (EUDI wallet).

Since 2011, ACN has been keeping an exhaustive watch on the latest developments, particularly legislative, concerning digital identity in France development of strategic roadmaps, position papers and parliamentary hearings, ...

in innovative digital identity solutions. Its work Electronic and Communication Industries is designed to bring together public and private (Fédération des Industries Electriques, Electroniques players by strengthening coordination between the et de Communication - FIEEC), an associate member political and industrial concerned actors. To this of the Campus Cyber and an active participant in end, ACN draws up and promotes common industry the work of the Strategic Industry Committee positions on national and European regulations Comité stratégique de Filière - CSF) of the Security

CyberSecurity Organization (ECSO).











Members and partners of ACN

Digital identity Capacity approach

Members of ACN





























Certigna





ChamberSign [] (g | i d Conce





(Oralium









































KAT LEGAPASS







moment-tech nameshield



PRIVATE M CONTROL RANDURISEC





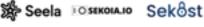














477























STOR O SYSDREAM Systancia THALES THE STREET STATES





















Partners of ACN



























OlGHIAL

SRICHARITY



