Programme
Associated Events
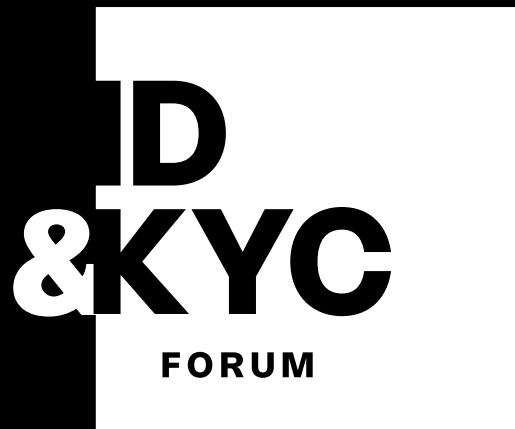
CF
CYBERSECURITY
FOR INDUSTRY

D&KYC
FORUM

TRUST &SAFETY
FORUM

W3S
WEB3
SECURITY
SUMMIT

CYBER INVESTOR DAYS

OSINT DAY

IN CYBER FORUM
EUROPE

26–28 MARCH 2024

LILLE GRAND PALAIS

ID &KYC

FORUM

INCYBER FORUM

EUROPE

26–28 MARCH 2024

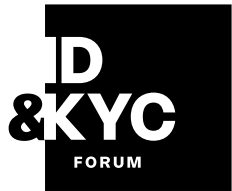**LILLE GRAND PALAIS**

2024 THEMES
The customer at the heart of technological change

Health, banking, transport, education, e-government… digital identity is now at the heart of economic activities and civic life.

Round Tables

Special 5th birthday ID&KYC Forum
Review and perspectives of digital identity (and KYC) in France and in Europe

On its fifth anniversary, the ID&KYC Forum invites several national and international personalities to speak on the results and prospects of digital identity. What has been achieved in France over the last five years? What were the failures and successes? Where does France stand in relation to the evolution of the European landscape and the progress made by its neighbors? How do different market segments use the solutions offered by the government and the private sector? What is the adoption curve by the public? What are the priorities for the next five years? Is there a consensus on these priorities?

"Anti-money laundering package" and new "European digital identity framework": what will be the impacts?

At the heart of the issues of digital identity and knowledge of customers and partners, two major European regulations follow parallel timetables and will in all probability be definitively adopted during our Forum. How will they impact business activity and societal-household life? How do these texts mark an evolution or even a revolution in customer relations practices and the distribution of digital services? Are there synergies and interactions between these regulations? What will be their respective and combined impacts? How to prepare for the arrival of the new rules? What are the accompanying texts and implementations? How to interpret them? What developments or updates should be expected for businesses?

Round Tables

Electronic wallet how to adjust to new intermediation strategies for tomorrow?

Today, more than one in two e-commerce transactions in the world are carried out via mobile phones. Through the provision of ergonomic simplicity, application security and a legal guarantee, the rise of electronic identity, payment and digital currency wallets creates a new intermediation capacity for transactions and services of tomorrow. How big is this development? Who will benefit from this new intermediation? What do businesses and financial services need to do to participate? Will European digital portfolio projects be able to compete with the digital giants? How do transactional ecosystems build ton banking/postal or telecom/sectorial networks using digital id* will cope with that? What are the societal consequences of this new form of intermediation?

"EUDI Wallet": which functions for promoting a new life on mobile?

Authentication, electronic signature, payment: what are the functionalities promised by the European mobile wallet (EUDI)? How will they relate to each other? For what uses? Halfway through the European pilots of the four consortia, what lessons have emerged? Digital services, travel, opening a bank account, professional identities: where are the most significant innovations located? What are the impacts on technical architectures? The "high" Security level of the European portfolio: how to understand it? how to implement it? how will it be used? What are the options? Will European citizens and consumers benefit from a new life on mobile with these journeys?

How to optimize digital journeys with KYC and AI, to improve customer engagement?

Data governance allows organizations to test and implement digital strategies. Customer Knowledge (KYC) tools and Artificial Intelligence (AI) techniques make it possible to go further, by combining proposals better calibrated in terms of risk and opportunities, and by improving the personalization of the service. What are the benefits of KYC automation and Artificial Intelligence on user experiences (UX)? How to combine the two approaches? What are the impacts on real-time data verification, customer enrollment, consent management and transaction monitoring? What is the feedback on the market?

Which are the pillars to build the digital identity of the future (2030–2050)?

Besides mobile wallets, what are the most structuring approaches for the digital identity of the future? We address several essential themes here. Digital Identity Infrastructure is a concept that considers that digital identity must be inserted into a broader "digital public infrastructure" approach (ITU/G20). The resulting ecosystem notably combines data exchange and transaction management, allowing digital society to function more optimally. Several approaches or architectural models can then be adapted (eg: decentralized, centralized, federated) for different applications. Identity & Attributes Trust Frameworks are sets of rules and standards to which trust operators can adhere and against which they can also be certified to demonstrate their ability to deliver data whose integrity and compliance are guaranteed. The Central Bank Digital Currency (CDBC) has progressed, like the European digital currency or the Swedish e-krona. However, it still faces the need to be able to identify people and/or accounts effectively before it can be implemented for the public.

Round Tables

Improving the fight against digital fraud in consumption, identity, and payment

Inflation and the increase in the cost of living have led several European authorities and organizations (EUROPOL, EBA, EPC, CIFAS UK) to warn against the proliferation of threats of scams and cyber fraud penalizing consumers. in their purchase, payment, or service transactions. Identity thefts, online or telephone manipulation, scams, false commercial offers, spyware, hacking and data interceptions, the risks are everywhere.

What are the most targeted transactions? What are the goals of fraudsters? How can we better detect fraud and prevent threats? Who to alert and what are the possible remedies? How to manage relationships with customers in a context of high risks? How to strengthen the culture of risk and fraud management within companies? What are the feedbacks and best practices to put in place?

IAM–CIAM: increasing data fluidity through identity orchestration

More fluidity and less friction for users: this seems to be the motto of corporate identity management today. A practice which affects all internal and external customers of the company: employees, partners, customers, non-human entities such as applications or connected objects. Thanks to orchestration platforms, not only are the company's different audiences onboarded, authenticated, and supported in authorizations, but they also free themselves throughout their digital journeys, from the complexities of the various IT environments.

Without programming, without effort, without passwords, how can identity orchestration generate fluid management of company data? How are user interfaces, connectors and APIs managed? Which parts of the life cycle can be automated and according to what criteria? How do management event notifications automatically reprovision identities and access? What are the profits according to the size of the companies?

Round Tables

Trust of business organizations and professional identities: a breath of modernization

Driven by electronic invoicing, digital signatures and the development of transnational exchanges, the digital identities of companies and professionals are the subject of intense work of reflection with a view to modernization and increased interoperability. While respecting the very strict security requirements, new possibilities are emerging for the management of the trust attributes of companies and professionals: company registers, professional e-wallets, certification schemes, solvency information, management of mandates.

What are the structuring initiatives? What legal confidence should be given to digital identities? What are the developments in the management and use of business registries in France and Europe? Who are the stakeholders in this evolution? How will digital certificates evolve? Will the digital identity of organizations move from concept to reality? What are the next steps?

Towards more accountability in the use of the Internet, social networks, and platforms?

While online societal life has taken on an essential dimension, initiatives are progressing to better secure online digital services, clarify the content of offers and better protect children and teenagers from manifestations of hatred, pornography, and violence. In the United Kingdom, a new law called the "Online Safety Bill" (OSB) aims to make the United Kingdom "the safest place in the world for the Internet". Strong measures have been taken to protect children and make platforms responsible for hosted content. In France, the bill aimed at securing and regulating the digital space (SREN) has very similar objectives in the fight against online scams and in child protection. European DMA, OSB, SREN: will the new legislative and regulatory framework finally support more responsible use of the Internet? How will we be better protected online? What are the obligations for online platforms and services? What certification practices will be used? What measures are taken for age verification? What role will digital identity play in making the Internet more secure?

INCYBER FORUM

EUROPE

26–28 MARCH 2024

LILLE GRAND PALAIS

Contacts

partnerships

partenariat@forum-incyber.com

programme

programme@forum-incyber.com