Workshop outcomes: Online Workshop on
Identity Attributes and KYC: the Transition to eIDAS 2.0 and AMLR era
16 September 2021

The objective of the **GRIDS-eIB joint workshop** was to inform policy-makers and industry stakeholders on the latest policy developments in the area of eID, remote identity management, KYC and, more generally, on identifying critical technology needs and design principles for emerging decentralized technologies.

grids
INCREASING TRUST WITH EID FOR DEVELOPING BUSINESS

eIB
eIDAS enabled i-banking

GRIDS and eIB projects are funded by CEF Telecom

Co-financed by the European Union
Connecting Europe Facility

Video: You can re-watch the video of the workshop at any time using the following link: https://drive.google.com/file/d/19YFxdwzMkHGtxXWr4d3YEN8UvR7Bl5O0/view?usp=sharing

Summary: After the necessary introductions by the host, **Petros Kavassalis** (University of the Aegean, Greece), **Juan Carlos Perez Baun** from ATOS Spain (Research and Innovation) introduced their involvement with state of the art eID projects. The importance of trust in order to exploit the full possibilities and compliance needed with AML and other regulations that establish strict KYC needs was addressed as well as how ATOS were among the pioneers in this field, including via their participation in the GRIDS project.

Next, **Romano Stasi**, Managing Director of ABI Lab (Italy), discussed the latest practices in the Customer Digital Onboarding landscape in the banking sector. Subsequently, Data from the Italian banking sector were presented that made clear how the majority of banks in Italy intend to provide (or already do provide) digital onboarding for prospective customers in the near future. How this observation becomes especially interesting was also discussed, in conjunction with the newly proposed eIDAS 2.0 regulation, which specifies user controlled applications (wallets) for the handling of personal identification information and beyond.

With this in mind, **Michal Hrbaty**, from the European Commission (DG CNECT), explained how a single digital identity for all citizens is envisioned and proposed to be designed in the context of the recent proposal for the European Digital Identity framework[1]. Specifically, the need for a new form of pan-European Digital ID framework was made evident by the facts presented. How the current eIDAS regulation has shown limitations on delivering its goals, for example by the fact that only a few of MSs have notified national eID schemes under eIDAS until now, and the uptake by the private sector is relatively low. Additionally, it was noted that the EC is seeing significant push and potential for ID platforms that utilize Digital Identity wallets and are capable of expanding to other policy areas, such as finance, transport, health, etc. Due to these reasons the new revised Regulation is based on three pillars, as explained: Strengthening of the national eID systems under streamlined eIDAS notification procedure, involving the private sector as Providers of identity linked services and finally enabling user controlled exchange of digital identity data and linked credentials via Personal Digital Identity wallets. Under the new Regulation, Member States will provide digital wallets to their citizens, residents and businesses that they could complement with attestations in such a way that it enables relying parties to check their validity and at the same time provide citizens the option of selective disclosure of their attributes.

[1] Announcement of EU common eID (eIDAS 2,0) : 26 May
European Digital Identity | European Commission (europa.eu)

Next, **Emiliano Anzellotti**, from the ECSA (European Credit Sector Associations) e-ID Task Force Co-Chair, discussed the deficiencies in terms of interoperability of existing standards and additionally on the availability of notified eID schemes across the EU. The barriers to entry for the private sector were additionally discussed. It was explained that for these reasons the ESCA created a special task force to address these issues with experts from the EU banking industry. During the presentation, it was explained how crucial it is for the uptake of such systems that the eID is something citizens can use frequently, for many purposes, and not only 1-2 times per month. Also, it was pointed out, with respect to the new eIDAS 2.0 regulation, that the need for cooperation and fine tuning between the private sector and the EC is very important before the final text of the regulation is agreed. The most pressing issues that need to be discussed with this respect is the need for clear liability chains, and the cooperation between private sector and MS in the creation of the European Digital Wallet to ensure interoperability with other financial apps.

Continuing, **Stephane Mouy** (SGM Consulting & ETSI, France) presented a preliminary design for a digital identity wallet like the one envisioned by the eIDAS 2.0 regulation. It was also explained that the requirements for such wallets is a challenging task, technically speaking. They need to meet High LoA requirements, the user needs to be in full control of their wallets, issuers need to attest the attributes and securely transmit them to these wallets and, on top of that, wallets should support qualified electronic signatures. Finally, these wallets will have to be accepted by everyone, work online and offline and support payment authorizations. Apart from these features, they should protect the user's privacy, enable the user to maintain multiple identity profiles (social, business, etc.) and prevent user traceability. It was explained that for these reasons the unique eIDAS 2.0 identifier requirement is becoming a hot topic for discussions across the EU -- and the discussion made evident the need for a clear privacy-safeguarding approach. Next the flows of such a wallet implementation were described and **Michael Adams** (Quali-Sign, UK), presented in detail a working demo of an open wallet proposal meeting eIDAS 2.0 requirements. The proposed wallet is in the position to manage attributes received by various Attribute Service Providers (issuers) and communicated to Relying Parties, with Identity Service Providers responsible for the identity binding/proofing. The wallet operates under the full and sole control of the user, who decides which attributes are communicated to Relying Parties. Each attribute stored is evidenced by a cryptographically signed digital (qualified) attribute certificate which securely identifies its issuer as well as the attribute details, and can be verified by each Relying Party. All attribute certificates reference an (qualified) identity certificate, which serves as 'wallet anchor'. SCA is performed on all eID transactions conducted through

this wallet (including payment dynamic linking). The eID proof takes the form of a qualified electronic signature.

Chiara Bacci, from the European Commission (DG FISMA), gave an overview of the proposals setting up the new EU anti-money laundering and counter-terrorism financing framework[2], with a focus on Customer Due Diligence. She explained that this recently announced updated AML package harmonises CDD (Customer Due Diligence) across the EU and clarifies the factors and variables for the evaluation of risk which will define the intensity and extent of CDD. The harmonization of CDD requirements should facilitate the use of digital identity in the financial sector, especially in customer onboarding and cross-border service operation. The proposed changes to the AML framework are in line with the proposal of the Commission for a common EU digital eID (revised eIDAS proposal[3]) and further specify issues related to identity verification and authentication for remote on-boarding purposes. The (reliable) data sources for identification and the necessary attributes required in the context of the identification process in order to achieve a standard, simplified and enhanced due diligence will be defined through regulatory technical standards (to be issued by the envisaged EU AML authority (AMLA) -- the new package outlines an integrated EU AML supervisory system and establish an EU AML authority (AMLA) in the form of a decentralized regulatory agency.

Continuing, **Peter Bainbridge-Clayton** (360kompany, Austria) presented the GRIDS project in detail and in particular how the GRIDS architecture aggregates access to all business registers through one platform and API proving it came from a primary and provable source. GRIDS offers solutions that bundle cross-border individual and business verification services under one roof. The main goal of GRIDS was clearly presented through three different use cases. They enable natural persons with an eIDAS eID, representing business companies (i.e. an individual granted with a mandate to represent a legal person), to be able to go to a European bank and open a bank account, for the company they represent in a much slicker way; or, to apply to an LEI issuer for a LEI to be issued to a company they claim to represent, or to transact with a Legal Services Provider etc.. In all these cases, GRIDS acts as a trust source in the sense that it allows the Service Provider (in the above example, the Bank opening an account, the LEI Issuer or the Legal Services Provider): a) to contact the Data Provider(s) it chooses directly to perform the KYB lookup and, b) to validate the

[2] AML adaptation to remote identification and verification: 20 July
Anti-money laundering and countering the financing of terrorism legislative package | European Commission (europa.eu)

[3] Announcement of EU common eID (eIDAS 2,0) : 26 May
European Digital Identity | European Commission (europa.eu)

identities of the person and the company, and the claimed relationship. All this is achieved through the KYB attributes (i.e. company information obtained from official primary sources around the world) which may not be directly part of the current public debate on digital identity management, but play a big role in everyday business. The key role of eIDAS to the KYC/KYB business network of GRIDS, which is an emerging private sector-driven ID platform for decentralized business identity management, to leverage all the regulatory advantages of the eIDAS Network was also explained.

Eric Wagner (Raiffeisenbank International AG, Austria), analysed the existing synergies and dependencies between the emerging eID ecosystem and the under development Central Bank Digital Currency (CDBC). At first, the potential risks of CDBCs were discussed and how these can be mitigated by designing CBDC to be account-based/ID-verified. Next, an overview of how Big Market Players (MasterCard, Visa, Paypal, etc.) started positioning themselves in the Crypto Asset/CBDC area, has been given. Continuing, it was analyzed how eID wallets (like the EDIW) can complement CryptoAsset wallets to enable a simplifying user experience, help to define open standards, enable Data Privacy and minimization, and finally support broad ecosystems spanning over public and private constituents. Four emerging trends were presented in detail then: Trend 1 - Simplify User Experience by combining CryptoAsset and eID, Trend 2 - Use Open Standards and Trust Framework to avoid monopol/oligopol lock-in, Trend 3 - Data Privacy and Minimization bydesign to avoid traceability and maximize Data Protection, Trend 4 - Support a broad ecosystem across all relevant public and private sectors. Closing, the speaker discussed how these features can be supported via a chain of countersignatures supporting offline root-of-trust (and hints towards equivalent Verifiable Credential based solutions).

Ralf Ohlhausen, (PayPractice, ETPPA, PPRO, Tink, Germany), proceeded to discuss online and offline SCA (Strong Customer Authentication), explaining why offline interactions, where a user's wallet does not need an Internet connection for payments, are important and how these can be achieved using the so-called "embedded approach". He presented: a) the principles this type of authentication should adhere to, most of which were defined within the Berlin Group Advisory Board Project "Signed Payment Request" with the objective to improve the user experience and security of the SCA procedures, and b) the opportunities and use cases it enables with respect to both payments and other types of interactions using identity wallets (among them: secure storage of attributes/credentials, bound to an identity and a device, e.g. digital certificates, identifying a Relying Party to answer only legitimate requests, presenting and potentially combining only a subset of stored attributes to the Relying Party using an offline chain of trust, etc). This will allow banks to accept the European Digital Identity Wallets (EDIWs) for SCA as required by the eIDAS 2.0 proposal.

Following, **Nikos Triantafyllou** (Univ. of the Aegean | i4m Lab, Greece), presented how in the scope of the new eIDAS 2.0 wallet based identity (EDIW) ecosystems, RegTech KYC/KYB providers can reinvent themselves (or enable others to) become KYB Verifiable Credentials Issuers. Verifiable Credentials (VCs) are proof that you know something or have something. They can be issued by a trusted entity, about anything, and can be instantly verified by everyone. VCs are at the core of Self Sovereign Identity (SSI) which may have influenced the core principles of the recently proposed eIDAS regulation update. It was explained how VCs cryptographically: bind the identity of the issuer of the credential, ensure that they were issued to the entity presenting them, are tamper resistant, and finally ensure that they have not been revoked. VCs, and VC-enabled business wallets, may potentially become an effective vehicle for a minimal KYC/KYB facility which will implement the requirements for remorse identification of the recently proposed by the Commission AML package, In this context, it was discussed how the potential transformation of KYC/KYB providers to VC Issuers, or the establishment of new players acting as Identification Service Providers for remote identification with traditional DCs (banks, telecoms etc.), under the eIDAS 2.0 EDIWs, can enable the creation of a portable KYB identity company, and how that profile can be efficiently managed and used to enable seamless access to FinTech services. GRIDS has the intention to propose such a generic case-example of an ID platform that utilizes a Digital Identity wallet for the needs of the SMEs and other business companies.

Luca Boldrin (InfoCert, Italy), proceeded with an overview of the discussions thus far. He identified three main points: i) The importance of merging identity and payment transactions, and how SCA (Strong Customer Authentication) in the embedded flavour may be the key to this goal. ii), The importance of creating wallets for companies and not only for natural persons, since most of the KYC value lies there. iii) The availability of different technologies (W3C, X.509…) which can respond to the same requirements, even if the different maturity levels should be taken into account. Essentially, it was remarked that adoption equals usage and, and to achieve high adoption rates, we should leverage on the traction from payments, possibly by merging identity and payment wallets. According to Luca Boldrin, this emerges as one of the major conclusions of the Workshop.

Closing, **Marie Markosian**, Financial Innovation and Digital Policy Advisor of MEP Eva Kaili, noted that the workshop was interesting for both those involved in policy making and those in the development of tech solutions as it offered a holistic perspective and approach on how digital identity should be built and safeguarded in the near future. It was also stated that, as the digitalisation and delocalisation of processes have created unique opportunities and risks alike, including sophisticated money laundering and terrorist financing techniques, it is of utmost importance for businesses to deploy solutions for digital identification supported by artificial intelligence and machine learning

that will utilize data intelligence and smart technology, such as predictive algorithms, etc., to automate data assessment, detect stolen IDs and deep fakes.

Table: Questions & Answers during the workshop

No	Question	Answer
1	What is the indicative budget for GRIDS and for eIB? L. 2:17 PM	1M for eIB, 1.16 M for GRIDS
2	As SCA in Payment is for security reasons based on dynamic factors (logic in chips, calculations of Hashes, Counter for maximum offline usage) there are technical issues with an ID wallet system with "static credentials" too, am I right? Just from a technical view. J. 2:32 PM	Hello J., thank you for your question. The ID wallet can use a cryptographic private key (for the possession element) combined with a PIN (knowledge) and/or Biometrics (inherence). The wallet can perform dynamic linking including display of the payee and amount and generation of the authentication code (electronic signature) linked to payee and amount. I hope this makes sense.
3	Is there the possibility to have more than one Wallet in a MS? (Example: one issued by MS and one independently but recognized by MS). E. 2:46 PM	Hey E., again I am not part of the eIDAS 2.0 committee but if I recall correctly from my last read of the proposition you are correct, you can have multiple wallets per MS. I hope it helps. 3:38 PM
4	Maybe a dumb question, but is there web page for this "e-wallet network"? V. 3:00 PM	Not yet unfortunately - work in progress...
5	Do I understand correctly: in the cross-border setting, eID attributes from the wallet will not be "shared" from Citizen to Service Provider via the existing eIDAS Interoperability framework(MS Nodes)? and interoperability is planned to be achieved via mutually recognized set of standards among MSs? J. 3:02 PM	Hey J., not part of the regulation but from my latest read of the eIDAS 2.0 proposition yes this is the case. User store attributes in their EDIW which they then disclose themselves to the services providers. So the existing eIDAS network should not be necessary any more. At least, that is my understanding. I hope it helps until someone more qualified answers. 3:37 PM
6	Is there source code or other documents for these demos? V. 3:28 PM	Hello V., yes the demos are available here: https://www.quali-sign.com/resources_demonstration_evaluation.html
7	The Relying Party (RP) lists the	Hi J.. The Relying Party signs every

	attributes that they require ==> But that would mean, if a relying party like banks want to offer / use different use-cases, it needs to have more than one qseal, at least one for each use case. Should be kept in mind during the toolbox work. J. 3:44 PM	request to each EDIW. So every request can contain a different list of required attributes. Agree this needs to be kept in mind for the toolbox. We have included the idea that some attributes are mandatory (i.e. the bank can't open the account without them). Others are optional and if the user does not want to share them, they can still proceed. The relying party signs each request with their QSEAL Certificate (and the corresponding private key).
8	Technical infrastructure (i.e., channel - messaging service? etc.) via which list of eID attributes are exchanged, is provided by the Relying Party (bank in this case)? B. 3:35 PM	Hello B. The Relying Party (RP) lists the attributes that they require. This list is included in the RP's signed (qseal'd) request. The messaging/communication options include HTTPS and proximity connections (e.g. BLE). All messages are end-to-end encrypted using the Diffie-Hellman (ECDH) standard.
9	Does anyone know this article, or have a link to, of Eric's he mentions about the identity? V. 4:30 PM	Hi V. Eric has written a number of papers on CBDC. Here is a draft copy of one we collaborated on: https://www.quali-sign.com/documents/integrated_cbdc_eid-21-02-07_draft_pending_publication.pdf
10	Hi all, if I am not mistaken, in the grids, it seems that if we wrap an eidas connection and a kwc claim in a w3c credential, a wallet job is done, right? P. 4:24 PM	Hey P. That is kind of the topic of my talk later on.
11	Compared to TruAge from NACS, how different is this? https://www.brewbound.com/news/nacs-announces-truage-digital-id-verification-solution-supported-by-molson-coors/. M. 4:50 PM	In EDIW, a "proof of age" takes the form of an attribute attestation. The attestation is essentially a verifiable credential that is signed by the attribute issuer. There is a lot of talk about W3C and VC's. The demo you saw earlier uses X.509 Attribute Certificates (instead of the VC) and ETSI XAdES Qualified Electronic Signatures (instead of the VP). The benefit is it has an offline chain of trust that can be verified offline. W3C currently does not work offline.

12	The NACS Truage solution is using W3C VCs and does work in an offline mode. M. 4:59 PM.	Hi M. Interesting! Can you explain how each party (wallet or terminal) can authenticate the other offline using W3C? I.e. it needs a local copy of the chain of trust that is normally stored in a Distributed Ledger in the W3C model.
13	I believe it is using either did:peer or did:key for the anchoring. It is integrated into the existing PoS's in the retail store, so no additional equipment is needed.	Can you explain how these map to real world identities which can be used to authenticate the signer whose signature can be independently verified offline?

The workshop was organized jointly from the GRIDS project and eIB project. GRIDS and eIB projects are funded by CEF Telecom and will be implemented from April 2019 to December 2021.

Speakers' short CVs:

Petros Kavassalis is the Dean of the Engineering School of the University of the Aegean and Director of the i4m Lab | UAegean.

Juan Carlos Perez Baun is GRIDS project coordinator. Researcher in the Blockchain, Identity & Privacy Unit of Atos Research and Innovation department.

Romano Stasi is Managing Director of ABI Lab, the Italian banking research and innovation centre. He is also founder and Director of CERTFin, the national centre of excellence on cyber security for the banking sector,

Michal Hrbaty is Legal and Policy Officer at the European Commission (DG CNECT) involved in the implementation of the eIDAS framework and its revision process concluded in the proposal on the EU digital ID framework.

Chiara Bacci works as a policy officer in the European Commission's (DG for Financial Stability, Financial Services and Capital Markets Union). Chiara is part of the team dealing with the EU anti-money laundering framework and the supervision of EU obliged entities.

Emiliano Anzellotti is the co-Chair of the ECSA TF (EBF, ESBG, EACB) that is following the eIDAS 2.0 discussion.

Peter Bainbridge-Clyton is the CTO and co-founder of 360kompany AG.

Mag. Dr. Eric Wagner is product owner of anti-money laundering and sanctions at Raiffeisenbank International AG. In that role, he is responsible for building a next generation aml and sanctions services platform based on big data and machine learning platform. Furthermore, he is engaged in numerous international, European and national expert and working groups covering financial crime, electronic identity and KYC, advanced analytics and technologies such as big data, artificial intelligence/machine learning, network analytics, natural language processing, distributed ledger technologies and quantum computing.

Stéphane MOUY is the founder and president of SGM Consulting, a digital transition consultancy focusing on e-trust services and eKYC processes for the financial services sector. He was an in-house attorney for BNP Paribas until 2018, working on electronic money schemes and on data protection/GDPR compliance as well as on several digital identity and remote onboarding initiatives for retail services. In 2021, he was involved in the ETSI task force preparing technical specifications for remote identity-proofing processes for trust services and is a contractor for DG FISMA of the European Commission focusing on KYC portability within the financial sector.

Ralf Ohlhausen is the founder of PayPractice advising Payment Service Providers, notably PPRO and Tink, with a focus on Open Banking. Previously, he was Chief Strategy Officer at PPRO and President Europe for SafetyPay. Prior to that, he spent 10 years each in telecoms and IT. Ralf chairs the European TPP Association (ETPPA), co-chairs the Berlin Group's openFinance Advisory Board, and is a member of the ECB's Market Infrastructure Board as well as an alternate member of their Euro Retail Payments Board (ERPB) and the board of the European Payments Council (EPC).

Luca Boldrin, PhD, presently investigates innovation trends and manages research initiatives for InfoCert, the largest EU qualified trust service provider His core competences are on trust services, identity management, distributed ledgers, security. He has been involved as a subject expert in many digital transformation projects, both at national and international levels, and regularly takes part in standardization initiatives in his areas of expertise. He is a member of the EU Blockchain Observatory expert group.

Michael Adams is the founder of Quali-Sign Ltd., specialists in mobile apps for eID and PSD2 SCA. Michael's background includes IBM and Barclays, where he managed the corporate bank's host-to-host payments channel. In recent years, Michael has participated in the UK and Berlin Group Open Banking forums and EU/UK forums on

Electronic Identification (eID). Michael is also currently a member of the Bank of England's CBDC Technology Forum. Quali-Sign has supplied a demo recording to the European eIDAS enabled i-Banking project.

Nikos Triantafyllou is a senior researcher with the University of the Aegean | i4m Lab, with significant experience in software engineering specifically in the fields of e-identity management systems (eIDAS eID enabled applications and self sovereign identity technologies). He received his Ph.D. in Formal Methods from the School of Electrical and Computer Engineering of National Technical University of Athens (NTUA). His interests focus on the fields of Information Management and Security, Privacy by Design, Blockchain and Decentralized architectures, Federated identity Management systems and the use of Formal Methods in eIdentity Systems Engineering. In the last years he has participated in both the design and implementation of several research and innovation projects enabling ecosystem development around eIDAS eID (ECAS, LEPS, ESMO, TOOP, GRIDS), and is the lead SSI architect of the SEAL project (Student Linked Identities).

Marie Markosian is an experienced Hellenic Capital Market Commission auditor, skilled in Capital Markets legal framework, FinTech, and Digital Economy. She was the coordinator of the HCMC Innovation Hub and appointed representative at the European Forum for Innovation Facilitators (EFIF). Currently, she is Policy Advisor to MEP Eva Kaili, connected to the ongoing process of multiple pieces of legislation in the fields of Fintech/Digital Finance, Platform economy, AI and Big Data.

About GRIDS and eIB projects

GRIDS (increasinG tRust with eId for Developing buSiness): GRIDS aims at simplifying the online remote onboarding of individual and business customers, mostly SMEs,. It specifically allows business platforms to enlarge their customer base across borders providing access to a secure digital environment where transaction participants are reliably identified and authenticated. GRIDS provides electronic one-stop-shop solutions for a complete and accurate KYC screening -- including not only company information and documents (name, register number, country/jurisdiction, court or legal form) but also the identification of natural and legal persons through effective access to the cross-border functionalities of a well-established eID DSI and eIDAS core service platform.

eIB (eIDAS enabled i-banking): eIB aims at developing a business process model for automating the process of opening a new customer and bank account cross – border. It will design and develop a new generation of cross-border e-banking services by creating an eIDAS enabled value chain, an "i-marketplace", where a Bank and Retail Service Providers (operating in different locations across the EU) collaborate in real-time to identify users with high level of assurance, via their eIDAS identifiers, exchange assets and information and ultimately offer banking products and automated e-services.

All partners involved in these projects are committed to continue supporting the architectures, services and policy guidelines developed during these programmes. The results of GRIDS will be piloted with the collaboration of influential EU FinTech companies (under the guidance of 360kompany and ATOS). These results will help further mature the infrastructure built by GRIDS and will ensure its uptake from the industry. Additionally, the effort undertaken in GRIDS will help to bring the importance of KYB to the spotlight and introduce them into the policy makers agenta, thus extending the current public debate which mostly focuses on KYC. The results of eIB will be utilized for evidence-based policy making in the area of digital identity verification in the financial sector.

GRIDS and eIB projects are funded by CEF Telecom

Co-financed by the European Union
Connecting Europe Facility