Authenticated Anonymity Architecture (AAA)

Legal report

Authors:

Monica Palmirani, University of Bologna

Chantal Bomprezzi, University of Bologna

Ludovico Papalia, University of Bologna - University of Camerino

Date: June 30, 2025

Version number: 1.0

Authenticated Anonymity Architecture - Legal report, 30/06/2025

Table of contents:

1. Introduction to the Authenticated Anonymity Architecture (AAA)

1.1. Objectives and context of the proposal

The Authenticated Anonymity Architecture (AAA) is a blockchain-based solution designed to address the fundamental tension between online anonymity and accountability in digital environments. The architecture seeks to establish a middle ground that provides robust anonymity for all legal uses whilst ensuring rapid and precise identification of anonymous individuals responsible for illegal acts, creating safeguards against governmental overreach. The AAA system operates through a network of national agencies, termed the Union of Identity Providers (UIP), whose members agree on technical and ethical baselines to ensure that only legally founded requests for deanonymisation are fulfilled. The architecture employs authenticated anonymous identifiers: anonymous accounts connected to the real identity of their owners in a manner that remains robustly concealed until a criminal act is performed using an account connected or created with those identifiers

The technical architecture comprises two distinct layers with different confidentiality levels: the secret layer, where data is retrieved and managed only by the owner through cryptographic systems, and the confidential layer, where data is collaboratively managed with each participant responsible for securely storing and protecting the data. The blockchain primarily serves as a secure, public, and distributed data storage mechanism, whilst smart contracts execute and manage all system operations in a secure and reliable manner.

1.2.Key legal aspects

The legal framework surrounding the AAA presents several critical considerations. The architecture must navigate the complex intersection of digital identity rights, data protection requirements, and law enforcement needs while, at the same time, maintaining compliance with European Union legislation. Central to these considerations is the fundamental right to digital identity, which has evolved from theoretical discussions to become increasingly relevant from a legal perspective. Furthermore, compliance with legal safeguards ensures that anonymity is preserved for lawful uses while enabling identification only through legally founded procedures.

1.3.Key ethical aspects

The ethical dimensions of the AAA are equally significant. The architecture must balance the legitimate need for anonymity in democratic societies with the imperative to prevent misuse for criminal purposes. Online anonymity serves crucial functions in protecting freedom of expression, preventing pressures from different parts of the society, and safeguarding against oppressive policies from authoritarian states. However, it also provides potential shields for cyberbullying, fake news dissemination, money laundering, and other illicit activities.

The ethical framework must address the risk of governmental overreach whilst ensuring effective law enforcement capabilities. The AAA's consensus mechanism, requiring agreement among multiple UIP members for deanonymisation, serves as a crucial ethical safeguard against abuse by individual actors or coalitions of oppressive countries attempting to deanonymize political opponents.

1.4.Sovereignty and Jurisdictional Issues

The AAA system operates through a network of national law enforcement agencies. Identities are legally and unequivocally linked to individuals, thereby ensuring both the anonymity of individuals with respect to external parties, and the ability of law enforcement to identify individuals during investigations and the prosecution of crimes.
The use of non-repudiable blockchain records to store deanonymization requests ensures that unscrupulous or rogue law enforcement agencies cannot deanonymize anonymous identities without appropriate warrants and sufficient evidence of illegal activity. Naturally, only legally justified requests for deanonymization are fulfilled.
Since the AAA architecture is intended to be adopted by multiple national authorities cooperating in a multinational context, the legality of any authorization to disclose identities for prosecution must be assessed in accordance with national legal systems—particularly criminal law and private international law (which determines the competent jurisdiction and applicable law when deciding whether, and by whom, the identification of an individual may be lawfully requested).
Thus, the decentralized consensus mechanism does not infringe national sovereignty by enabling collective decisions from multiple providers located in different countries. On the contrary, decentralization should be understood from a technical standpoint. In this respect,

technical decentralization not only safeguards but also reinforces national sovereignty by ensuring that only authorized entities can access individuals' real-world identities.

2. Legal Framework Overview

2.1. The right to anonymity vs illicit prosecution

Over time, the concept of personal identity has moved out of purely theoretical discussions, becoming increasingly relevant from a legal perspective. Indeed, courts and legal experts began to conceive personal identity as a person's right. This process cannot yet be said to have stopped. In particular, the advent of the Internet and the exponential growth of modern society has led to the concept of digital identity, which refers to the representation of people in the digital world. Thus, the concept of personal identity has evolved to encompass digital manifestations of personality that require legal protection. The European institutions have also emitted the "European Declaration on Digital Rights and Principles for the Digital Decade"[1] where "*People are at the centre of the digital transformation in the European Union. Technology should serve and benefit all people living in the EU and empower them to pursue their aspirations, in full security and respect for their fundamental rights*". In particular, the right to anonymity, whilst not explicitly enumerated in many legal frameworks, derives from broader privacy rights and freedom of expression protections. The European legal tradition recognises that anonymity serves legitimate purposes in democratic societies, enabling political dissent, protecting vulnerable individuals, and facilitating free expression without fear of retaliation.

However, this right must be balanced against society's legitimate interest in prosecuting illicit activities. The tension between digital identity rights and law enforcement necessities forms a central challenge for the AAA.

The AAA attempts to reconcile these competing interests by maintaining robust anonymity for legal activities whilst providing mechanisms for lawful deanonymisation when criminal acts are committed. This approach requires careful calibration to ensure that the threshold for deanonymisation is neither so low as to compromise legitimate anonymity nor so high as to frustrate legitimate law enforcement.

2.2. European blockchain strategy

The European Commission's blockchain strategy[2] establishes a comprehensive framework for blockchain deployment within the European Union. The strategy supports blockchain utilisation in adherence to European values and regulations, emphasising enhanced trust services, environmental sustainability, data protection compliance, digital identity integration, cybersecurity, and interoperability.

The Commission's approach recognises blockchain technology's potential to revolutionise information sharing and online transactions whilst maintaining strong regulatory oversight.

1 European Declaration on Digital Rights and Principles for the Digital Decade (2023/C 23/01), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOC_2023_023_R_0001.
2 https://digital-strategy.ec.europa.eu/en/policies/blockchain-strategy.

Initiatives such as the European Blockchain Partnership (EBS),[3] established in April 2018, and the subsequent European Blockchain Services Infrastructure (EBSI)[4] demonstrate the EU's commitment to becoming a leader in blockchain technology whilst ensuring compliance with existing legal frameworks. In particular, the EBP's vision is to leverage blockchain to create cross-border services for public administrations, businesses, citizens and their ecosystems to verify information and make services trustworthy.

In accordance with this path, the European Commission has set up the pan-European Blockchain Sandbox,[5] which establishes a pan-European framework for regulatory dialogues to increase legal certainty for innovative blockchain technology solutions. The regulatory sandbox approach allows for controlled experimentation with blockchain applications, enabling dialogue between innovators and regulators, where legal advice and regulatory guidance are provided in a safe and confidential environment.

This framework provides valuable insights for the AAA's development, as it must navigate similar regulatory challenges whilst pushing the boundaries of what is technically and legally possible in digital identity management.

2.3.Legal effects of blockchain and smart contracts

The legal recognition of blockchain and smart contracts forms a crucial foundation for the AAA's operation.

According to the EU Blockchain Observatory and Forum's Legal and Regulatory Framework report,[6] blockchains constitute electronic documents under eIDAS,[7] meaning that data contained therein, including smart contracts, cannot be denied legal force solely because of their electronic nature. These statements adhere to the international principle of non-discrimination laid down by the 1996 UNCITRAL Model Law on Electronic Commerce (MLEC), the 2005 United Nations Convention on the Use of Electronic Communications in International Contracts and enshrined in various EU regulations.

In this context, the revision of eIDAS Regulation[8] has recognised additional and peculiar legal effects for electronic ledgers (i.e., blockchains), defined as "*a sequence of electronic data records, ensuring the integrity of those records and the accuracy of the chronological ordering of those records*" (art. 3(52)). More specifically, it provides that "*an electronic ledger shall not be denied legal effect or admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form*" (Art. 45k). Legal effects vary according to the qualification of the

3 https://digital-strategy.ec.europa.eu/en/policies/blockchain-partnership.
4 https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/Home.
5 https://blockchain-observatory.ec.europa.eu/european-blockchain-sandbox_en.
6 EU Blockchain Observatory and Forum, Legal and Regulatory Framework of Blockchains and Smart Contracts (2019), https://blockchain-observatory.ec.europa.eu/publications/legal-and-regulatory-framework-blockchains-and-smart-contracts_en?prefLang=de.
7 Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
8 Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.

electronic ledger as qualified or not qualified. Electronic ledgers are qualified if they are provided by a qualified trust service provider and meet the requirements set under Art. 45l (art. 3(53)), compliance with which is presumed where such electronic ledgers meet the standards established by the EU Commission through implementing acts. Qualified electronic ledgers enjoy the presumption of the unique and accurate sequential chronological ordering and integrity of the data records they contain, (Art. 45k). A qualified electronic ledger provided in one Member State shall be recognised as a qualified electronic ledger in all other Member States, according to the mutual recognition principle. For "simple" electronic ledgers, presumption does not operate, so it will be up to the judge to evaluate the production of the above effects on a discretionary and case-by-case basis. The revision of the eIDAS Regulation has proven useful for identifying legal blockchain effects.

Smart contracts present challenges and opportunities for legal frameworks. Whilst they are not necessarily contracts in the traditional civil law sense, they may have legal relevance depending on their content and context. The distinction between smart contract code and smart legal contracts becomes crucial when considering their enforceability and legal effects. Art. 36 of the Regulation 2023/2854 on harmonized rules on fair access to and use of data (the so-called "Data Act"),[9] establishes some essential requirements regarding smart contracts (robustness and access control, safe termination and interruption, data archiving and continuity, access control, consistency with the terms of what the smart contract executes). Compliance with these requirements is presumed in the case of adherence to standards that the Commission or other European standardization organizations may draft. It should be noted that the rule holds value when such smart contracts are utilized for executing data-sharing agreements, and the concept of a smart contract is not necessarily tethered to an electronic ledger (recital 104). However, it serves as an illustration of the standardization of the smart contract phenomenon, with potential application in other fields.

2.4.Relevance of the eIDAS Regulation

To ensure that identities are legally linked with certainty to individuals, the project must take into consideration the provisions of the eIDAS Regulation. Indeed, the eIDAS Regulation provides the primary legal framework for electronic identification and trust services within the European Union.

The e-IDAS Regulation defines "electronic identification" as "*the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person*", while Art. 3(1)(2) states that "electronic identification means" is "*a material and/or immaterial unit containing person identification data and which is used for authentication for an online service*". The same Regulation also contains an obligation of mutual recognition of national electronic identification means among the Member States. The principle of mutual recognition establishes that every Member State can adopt its electronic identification means that must be recognized by the others (upon the

9 Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act).

respect of some preconditions laid down in Art. 6 of the Regulation). According to recital 9, mutual recognition is aimed to "*facilitate cross-border provision of numerous services in the internal market and enable businesses to operate on a cross-border basis without facing many obstacles in interactions with public authorities*", taking into account that "*in most cases, citizens cannot use their electronic identification to authenticate themselves in another Member State because the national electronic identification schemes in their country are not recognized in other Member States*". Electronic identification means can ensure low, substantial or high assurance levels according to technical specifications (Art. 8 of the Regulation).

Another instrument of identification is the electronic signature. According to Article 3(1)(10) of the e-IDAS Regulation "electronic signature" means "*data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign*". The Regulation recognizes three different kinds of electronic signature: the simple (Art. 3(1)(10)), the advanced (Art. 3(1)(11)), and the qualified (Art. 3(1)(12)). Only the latter is considered equivalent to a handwritten signature because of its higher level of reliability and trust (Art. 25(2)). In all other cases, the suitability of the document to satisfy the requirement of the written form can be freely assessed in court, having regard to its security, integrity, and immutability.

Electronic signatures concern natural persons. For legal persons, the e-IDAS Regulation disciplines electronic seals, which are '*data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity*' (art. 3(1)(25)). As for electronic signatures, there are three kinds of electronic seals: the simple (art. 3(1)(25)), the advanced (art. 3(1)(26)), and the qualified (art. 3(1)(27)). Qualified seals shall enjoy the presumption of integrity of the data and of correctness of the origin of that data to which the qualified electronic seal is linked (Art. 35(2)).

The recent adoption of the eIDAS 2 Regulation aims to overcome the limitations of the Regulation and accelerate the spread of electronic identity solutions across the EU. The final objective is the setting of a European Digital Identity framework. The revision adds the European Digital Identity Wallet to the list of electronic identification. It allows the user to store and retrieve identity data, including person identification data, electronic attestations of attributes linked to their identity, to provide them to relying parties on request and to use them for authentication; it also enables to sign by means of qualified electronic signatures and seal by means of qualified electronic seals (art. 3(42)). The peculiar characteristic of this wallet is selective disclosure, which empowers the owner of data to disclose only certain parts of a larger data set, in order for the receiving entity to obtain only information that is required (recital 59). Therefore, the wallet implements the so-called Self-Sovereign Identity (SSI) because it can store identity data that can be selectively disclosed.

Moreover, the eIDAS2 Regulation has introduced the so-called electronic ledgers, which have been discussed in more detail above.[10]

10 Par. 2.3.

For the AAA, eIDAS 2 Regulation novelties are particularly relevant. Indeed, the combination of EUDI wallet and qualified electronic ledgers may represent a secure and trustworthy way for selective disclosure of identity data.

2.5.Applicability of the General Data Protection Regulation (GDPR)

By its nature and object, the AAA architecture implies the processing of personal data. For this reason, ensuring compliance of the system with European rules on personal data (i.e., the GDPR) is of pivotal importance.

In this context, the relationship between GDPR and blockchain becomes relevant. While European institutions[11] have evidenced the opportunity to adopt blockchain-based solutions to preserve data integrity, enhance the control of citizens over the use of their personal data, reduce fraud and enhance transparency, the GDPR's application to blockchain-based systems presents significant challenges.

Key GDPR principles that impact the AAA include data minimisation, purpose limitation, storage limitation, and data subjects' rights. The immutability of blockchain records conflicts with the right to erasure (Article 17 GDPR) and the right to rectification (Article 16 GDPR), requiring innovative technical solutions to achieve compliance.

The AAA must therefore implement appropriate technical and organisational measures, including privacy-enhancing technologies, to ensure adequate data protection levels.

2.6. Interaction with the Artificial Intelligence Act (AIA)

As highlighted by scholars[12] and institutions,[13] there are several intersection points between blockchain technology and the AI Act.[14] The AAA may incorporate AI components for pattern recognition, anomaly detection, or decision support in the deanonymisation process, triggering AI Act compliance requirements.

Key considerations include the use of automated decision-making systems, which must comply with transparency and human oversight requirements. If the AAA employs AI for risk assessment or identity verification, it must ensure compliance with the AI Act's requirements for high-risk AI systems, including conformity assessments, technical documentation, and ongoing monitoring obligations.

11 Declaration on European Blockchain Partnership, European Parliament resolution of 3 October 2018 on distributed ledger technologies and blockchains: building trust with disintermediation.

12 C. BOMPREZZI, *Blockchain-based Smart contracts e e-Justice nella Proposta AI Act*, in M. Palmirani, S. Sapienza (a cura di), *La trasformazione digitale della giustizia nel dialogo tra discipline. Diritto e Intelligenza Artificiale*, Giuffrè, 2022.

13 European Blockchain Sandbox Best practices report 2nd Cohort.

14 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

The interplay between blockchain's immutability and the AI Act's requirements for system updates and corrections presents particular challenges. The architecture must design mechanisms that allow for AI system improvements whilst maintaining the integrity of the blockchain record.

3. Data Protection and Privacy Issues

3.1. Anonymity vs. pseudonymity in blockchain systems

The distinction between anonymity and pseudonymity proves crucial in blockchain contexts. As defined in the GDPR, pseudonymization involves processing personal data such that it can no longer be attributed to a specific data subject without additional information, provided such additional information is kept separately and subject to technical and organizational measures (Art. 4(1)(5)). Pseudonymized data remains personal data under GDPR, as it can be attributed to a natural person through additional information. True anonymization, by contrast, irreversibly prevents re-identification, removing data from GDPR's scope entirely.

In blockchain systems data are considered pseudonymous rather that anonymous.[15] Blockchain addresses serve as pseudonyms which, although they do not directly reveal real-world identities, can potentially be linked to individuals through transaction analysis, metadata correlation, or external data sources. Therefore, the AAA must carefully design its architecture to ensure compliance with the GDPR.

3.2. GDPR compliance challenges with blockchain

GDPR compliance challenges with blockchain present a complex interplay between technological capabilities and regulatory requirements that demands careful analysis and innovative solutions. Blockchain technology's inherent characteristics, particularly its decentralization, immutability, and append-only architecture, create fundamental tensions with core GDPR principles that require sophisticated approaches to reconcile. The principle of storage limitation, as articulated in Article 5 GDPR, mandates that personal data must be kept in a form that permits identification of data subjects for no longer than necessary for the purposes for which the personal data are processed. This requirement directly conflicts with blockchain's append-only nature, which creates an ever-growing ledger where data persists indefinitely (for mathematical definition, for the life of the ledger itself) and undergoes manifold replication across network nodes. The challenge intensifies when considering that blockchain's distributed architecture means that data deletion cannot be achieved through conventional means, as the entire network would need to coordinate such removal, potentially compromising the system's integrity and security properties.

The right to erasure, enshrined in Article 17 GDPR, faces the technical impossibility of removing data from an immutable blockchain register, is one of the most significant

15 M. Finck, *Blockchain and the General Data Protection Regulation – Can distributed ledgers be squared with European data protection law?*, Study of the Panel for the Future of Science and Technology (STOA), European Parliamentary Research Service, July 2019.

compliance challenges in blockchain implementations. This tension requires innovative approaches that achieve functional compliance whilst maintaining blockchain's security properties and consensus mechanisms. Some GDPR requirements may be challenging to implement in blockchain contexts but maintain that controllers must find innovative solutions rather than claiming technical impossibility. Where deletion has not been taken into account by design, compliance may require deleting the whole blockchain, an approach that fundamentally undermines the technology's value proposition. Alternatively, if the combination of on-chain and off-chain data compliance has been incorporated by design, it may be possible to prevent future identification of a data subject through erasure of off-chain data, depending on the exact architectural method chosen and the specific factual circumstances involved.

Data minimization becomes particularly critical in blockchain contexts, requiring controllers to demonstrate that blockchain represents the most privacy-preserving option available for their specific use case. The EDPB guidelines (see below) strongly recommend avoiding storing personal data on-chain where possible, instead advocating for off-chain storage solutions with on-chain references that maintain data integrity whilst preserving privacy rights. This approach allows for the benefits of blockchain verification and immutability without directly exposing personal data to the challenges of permanent storage. Where on-chain storage proves necessary for the functionality of the system, advanced cryptographic techniques such as zero-knowledge proofs, homomorphic encryption, or secure multi-party computation may provide privacy protection whilst maintaining the necessary functionality. The data minimization principle when viewed through the lens of blockchain implementation encompasses not only the quantity of data processed but also the level of publicity applicable to any personal data involved, requiring controllers to demonstrate that their chosen technique ensures only the minimum information necessary for processing is used with the minimum level of publicity exposure.

The determination of controller and processor roles in distributed blockchain networks presents additional complexity that extends beyond traditional data processing relationships. In blockchain environments, the GDPR's assumption that processors operate under clear contractual arrangements with identifiable controllers becomes complicated by the distributed nature of the technology and the potential for multiple parties to exercise varying degrees of control over different aspects of the data processing. The assessment of roles requires consideration of various elements, including the nature of the service provided, the blockchain governance mechanism, the precise legal, technical, and organizational characteristics of the blockchain implementation, and the relationships between different actors involved in the processing activities. The governance mechanism proves particularly important for determining roles and responsibilities under GDPR, as it defines the design model that could be centralized or distributed, registered on the blockchain or agreed upon separately, and establishes policies that may be technologically enforced or rely on organizational compliance.

In the AAA context, clear delineation of responsibilities among UIP members, node operators, and service providers becomes essential for GDPR compliance and liability allocation, requiring detailed analysis of how each party influences key elements of personal data processing. This includes assessment of roles in authentication and identification of users,

recording of data on the ledger including links to off-chain data, and verification of data integrity within the distributed system. The complexity increases when considering that different parties may act as separate or joint controllers at different stages of the process, necessitating comprehensive documentation of data flows and decision-making authority throughout the system's operation. The principle of accountability, as established in Article 5 GDPR, requires that wherever there is processing of personal data, there must be an identifiable controller capable of taking responsibility for GDPR compliance at every step in the process, a requirement that becomes particularly challenging in decentralized environments where traditional organizational boundaries and hierarchies may not apply.

3.3.EDPB Guidelines on processing personal data through blockchain technologies

The EDPB Guidelines 02/2025 on processing of personal data through blockchain technologies, adopted on the 8 April 2025**,** provide comprehensive guidance on achieving GDPR compliance in blockchain implementations. The guidelines emphasize the importance of data protection by design and by default, requiring controllers to demonstrate context-specific measures implementing data protection principles.

Key recommendations include conducting thorough Data Protection Impact Assessments (DPIAs) before implementing blockchain-based processing, implementing appropriate technical measures for data minimization, ensuring transparency for data subjects, and designing mechanisms to accommodate data subject rights within technical constraints.

The guidelines acknowledge that some GDPR requirements may be challenging to implement in blockchain contexts but maintain that controllers must find innovative solutions rather than claiming technical impossibility. This may require combining multiple privacy-enhancing technologies and implementing hybrid architectures that balance on-chain and off-chain processing.

As emphasised by the thematic report of the European Union Blockchain Observatory and Forum on Blockchain and the GDPR, compliance is not about the technology itself but about how it is used. There is no such thing as a GDPR-compliant blockchain technology; there are only GDPR-compliant use cases and applications.

4. Digital identity issues

4.1. Integration with legally recognized identification systems

The AAA must seamlessly integrate with existing legally recognized identification systems (see above 2.4) whilst maintaining its anonymity properties. This requires establishing trust bridges between traditional identity providers and the blockchain-based pseudo anonymous identity system. The architecture must ensure that the initial identity verification meets the standards required for the highest levels of identity assurance whilst preventing any linkability between verified identities and pseudo anonymous credentials during normal operation.

Integration challenges include accommodating varying national identity schemes with different security levels, document types, and verification procedures. The system must establish equivalence frameworks that ensure consistent identity assurance levels across different national systems whilst respecting local legal requirements and cultural considerations.

4.2. Compliance with the eIDAS 2 Regulation

The eIDAS 2 Regulation introduces significant enhancements relevant to digital identity systems. The European Digital Identity Wallet (EUDI Wallet) framework provides a model for user-controlled identity attributes that aligns with the AAA's privacy-preserving objectives. The regulation's provisions on electronic attestation of attributes offer mechanisms for conveying specific identity attributes without revealing full identity information.

Compliance requires adherence to technical specifications outlined in implementing acts, including standards for qualified electronic attestation of attributes services, security requirements for identity wallet providers, and interoperability specifications ensuring cross-border recognition. The AAA must ensure that its anonymous credentials can interface with the EUDI Wallet ecosystem whilst maintaining unlinkability between wallet-based identities and anonymous identities.

4.3.Integration with EU Digital identity framework

The EU Digital Identity framework envisions a comprehensive ecosystem where citizens control their digital identities across member states. The AAA must position itself within this ecosystem as a specialized service providing anonymous access where appropriate whilst maintaining compatibility with the broader identity infrastructure.

Key integration points include attribute verification services that can confirm specific characteristics without revealing identity, consent management systems ensuring user control over data sharing, and audit mechanisms that maintain accountability whilst preserving privacy. The architecture must balance the framework's emphasis on user control with the need for lawful deanonymization capabilities.

5. Ethical Considerations

5.1.Impact on fundamental rights and freedoms

The AAA's design profoundly impacts fundamental rights, particularly privacy, freedom of expression, and due process. The architecture must ensure that the availability of deanonymization mechanisms does not create a negative effect on legitimate anonymous expression. Citizens must have confidence that their anonymity will be preserved for all lawful activities without fear of arbitrary exposure. However, the temporal dimension of legal protection presents a more complex challenge that requires careful consideration within the AAA framework. The historical volatility of legal systems and the precarious nature of democratic freedoms demand recognition that activities considered lawful today may face criminalization tomorrow. Journalistic reporting, political criticism, whistleblowing, and

peaceful opposition, all fundamental pillars of democratic society, have repeatedly become targets of authoritarian legislation across different jurisdictions and historical periods. This reality could necessitate mechanisms within the AAA that can provide irrevocable anonymity for certain categories of expression that serve the public interest, even when such expression may later be deemed unlawful by shifting political regimes in an extended area, in an extreme case even in all the states parts of the consortium.

While maintaining the consensus-based deanonymization capability for genuinely criminal conduct, the system should recognize that certain forms of anonymous expression require absolute protection that cannot be compromised by future legal or political changes. This distinction becomes particularly crucial in protecting individuals engaged in activities such as documenting human rights violations, exposing corruption, or exercising political dissent in contexts where such activities may transition from legal to illegal based on political considerations rather than objective harm.

The system must also consider the rights of those accused of crimes, ensuring that deanonymization requests meet strict legal standards and that affected individuals have appropriate recourse to challenge such requests. The architecture should incorporate procedural safeguards preventing fishing expeditions or broad surveillance under the guise of criminal investigation, while simultaneously recognizing that the definition of "criminal investigation" itself may be subject to political manipulation in less democratic contexts.

5.2.Safeguarding the system from misuse for illicit purposes

With the finality of protecting legitimate anonymity, the AAA must implement robust mechanisms preventing its exploitation for criminal activities. This requires sophisticated monitoring systems that can detect patterns indicative of illicit use without compromising the privacy of legitimate users. The challenge lies in designing these systems to be effective against criminal abuse whilst remaining unable to conduct mass surveillance or profile lawful users.

Technical measures might include rate limiting to prevent mass account creation, behavioral analysis to identify suspicious patterns, and integration with threat intelligence systems to block known criminal infrastructure. These measures must be transparent in their operation and subject to oversight to prevent mission creep or abuse.

5.3.Safeguarding the system from surveillance abuse

The greatest ethical challenge facing AAA is preventing it from becoming a surveillance tool. The architecture must implement strong technical and procedural safeguards ensuring that the deanonymization capability cannot be abused for political persecution, mass surveillance, or social control and that States do not mechanically approve every request for de-anonymization in a tacit "do ut des" cooperation aimed at destroying the real anonymity that the system wants to provide.

Critical safeguards include the consensus requirement among UIP members for deanonymization, cryptographic protections ensuring that no single entity can bypass the

consensus mechanism, transparency requirements for deanonymization requests and their outcomes, and independent oversight bodies monitoring system operation. The architecture should also implement technical measures preventing the correlation of anonymous identities through traffic analysis or behavioral patterns.

6. Conclusions and Recommendations

6.1. Summary of key legal and ethical safeguards

The AAA navigates a complex intersection of digital identity rights, data protection requirements, and law enforcement needs, with the necessity to remain compliant with the European legal framework, particularly the GDPR and eIDAS regulations. Legally, the AAA preserves anonymity for lawful use but enables identity disclosure through strictly justified and auditable procedures. Ethically, the architecture seeks to balance the right to anonymity—crucial for freedom of expression and protection from surveillance—with safeguards that prevent misuse for illicit activities. The consensus-based deanonymisation mechanism, the use of pseudonymised identifiers, and adherence to privacy-by-design principles are essential pillars. Ultimately, AAA's compliance with evolving EU standards, such as the AI Act and the Digital Identity framework, ensures both legal robustness and ethical resilience in protecting user rights while allowing lawful accountability.

6.2. Policy recommendations

Considering the legal and ethical considerations discussed above, and based on the analysis carried out throughout this report, the following policy recommendations are proposed to guide the development and implementation of the Authenticated Anonymity Architecture (AAA):

The AAA system should ensure that identity disclosure is strictly limited to legally justified requests, processed through a non-repudiable, auditable mechanism involving a decentralized consensus among national law enforcement authorities. In a multinational framework, particular attention must be paid to respecting national legal systems, including criminal and private international law, to determine the competent jurisdiction and applicable legal standards. The technical decentralization of the system should be leveraged not only to preserve anonymity but also to reinforce national sovereignty, by ensuring that only properly authorized entities—within their respective jurisdictions—may access real-world identities.

The process of deanonymization must be strictly regulated and fully auditable. Deanonymization should only occur following a consensus among multiple members of the Union of Identity Providers (UIP), based on a multi-party, decentralized mechanism that ensures legal justification, non-repudiability, and traceability of all requests. The legal effects recognized for blockchain and smart contracts under the eIDAS 2 Regulation are crucial, and it is recommended to closely monitor the adoption of the implementing acts by the European Commission.

The AAA should be designed in strict compliance with the GDPR, taking into account the challenges related to the use of blockchain and the recommendations laid down in the recent EDPB Guidelines 02/2025 on processing of personal data through blockchain.
Furthermore, the AAA must take into consideration the European legal instruments of identity verification and ensure full interoperability with the European Digital Identity ecosystem, particularly the European Digital Identity Wallet (EUDI Wallet) introduced by the eIDAS 2 Regulation. Anonymous credentials issued or managed by the AAA must be able to interface technically with this infrastructure while preserving unlinkability between verified and anonymous identities under normal operational conditions.

In case of integration of AI components within the system, it is essential to ensure full compliance with the AI Act.

From an ethical perspective, robust safeguards must be put in place to prevent misuse of the deanonymisation capability for surveillance or political persecution. The system should employ cryptographic protections and procedural constraints that make it technically and legally impossible for any single party to unilaterally reveal an individual's identity. To this end, the adoption of a Code of Conduct is desirable.