future internet

MDPI

Article

Digital Identity in the EU: Promoting eIDAS Solutions Based on Biometrics

Pietro Ruiu [1,*], Salvatore Saiu [2] and Enrico Grosso [1]

[1] Department of Biomedical Science, University of Sassari, Viale Italia, 39/A, 07100 Sassari, Italy; grosso@uniss.it
[2] Department of Law, University of Sassari, Viale Mancini, 5, 07100 Sassari, Italy; salsaiu@uniss.it
* Correspondence: pruiu@uniss.it

Abstract: Today, more than ever before, technological progress is evolving rapidly, and in the absence of adequate regulatory frameworks, the big players in the digital market (the so-called Big Techs) are exploiting personal data (name, address, telephone numbers) and private data (political opinions, religious beliefs, financial information, or health status) in an uncontrolled manner. A crucial role in this scenario is played by the weakness of international regulatory frameworks due to the slow response time of legislators who are incapable, from a regulatory point of view, of keeping pace with technological evolution and responding to the new requirements coming from the social context, which is increasingly characterized by the pervasive presence of new technologies, such as smartphones and wearable devices. At the European level, the General Data Protection Regulation (GDPR) and the Regulation on Electronic Identification, Authentication and Trust Services (eIDAS) have marked a significant turning point in the regulatory landscape. However, the mechanisms proposed present clear security issues, particularly in light of emerging concepts such as digital identity. Moreover, despite the centrality of biometric issues within the European regulatory framework and the practical introduction of biometric data within electronic national identity (eID) cards, there are still no efforts to use biometric features for the identification and authentication of a person in a digital context. This paper clarifies and precisely defines the potential impact of biometric-based digital identity and hypothesizes its practical use for accessing network-based services and applications commonly used in daily life. Using the Italian eID card as a model, an authentication scheme leveraging biometric data is proposed, ensuring full compliance with GDPR and eIDAS regulations. The findings suggest that such a scheme can significantly improve the security and reliability of electronic identification systems, promoting broader adoption of eIDAS solutions.

Keywords: privacy; digital identity; Italian ID card; eIDAS regulation; facial recognition; biometrics; trustworthy digital environment

Citation: Ruiu, P.; Saiu, S.; Grosso, E. Digital Identity in the EU: Promoting eIDAS Solutions Based on Biometrics. *Future Internet* **2024**, *16*, 228. https://doi.org/10.3390/fi16070228

Academic Editors: Weizhi Meng and Christian D. Jensen

Received: 25 May 2024
Revised: 21 June 2024
Accepted: 24 June 2024
Published: 28 June 2024

1. Introduction

Technological progress has always shaped data protection and personal identity, with new profiles appearing in an incessant process, responding to new protection needs in the face of new dangers and threats brought about by technological development [1].

If, in the beginning (at the origins of the problem of the right to privacy), the pace of evolution was rather slow, so much so that it was compatible with the response time of an average legislator ready to grasp the new demands coming from the social context, the same cannot be sustained in the current era, in which regulatory acts run a strong risk of being born already unfit to respond to the continuous technological change [2,3].

The spread of a pervasive digital reality, which is increasingly destined to merge with the off-line one, in a bond in which the boundaries between one and the other tend to thin to the point of vanishing, and the absence of spatial references, conceived as physical places corresponding to the concept of territories, complicate the task of the legislator in no small measure.

Effective protection of the two fundamental rights protecting human personality, the right to privacy and personal identity, thus necessarily passes through an integrated approach between international, supranational, and domestic sources of law [4,5], accompanied by a rapid response to technological advances. From this point of view, the General Data Protection Regulation (GDPR) [6], which came into force on 25 May 2018 (replacing Directive 95/46/EC) [7], is the most important work of harmonization of the different national data protection laws existing in different EU Member States and has become a source of inspiration for other legal systems around the world, including the United States, e.g., the introduction of the CCPA—California Consumer Privacy Act, which came into force on 1 January 2020, which is a significant step for the United States in providing more rights to users and greater control over their personal data.

This context of recent contamination between different legal systems is enriched by numerous international agreements, treaties, and conventions that have established specific rules and regulations on the protection of personal data. Prominent among them is the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, first adopted in 1981 and recently updated in Convention 108+ [8] (adopted on 10 November 2018) precisely in accordance with an integration approach between legal sources, in order to address new challenges related to technological advances such as cloud computing, social networks, and big data.

1.1. The Questionable Role of the Big Techs

In the face of a challenge of global dimensions, in which powers other than the State, such as large digital market players (Big Techs), share with it de facto sovereign prerogatives [9], the recognition and protection of fundamental rights, precisely including privacy and personal identity requires a level of integration that must be as broad as possible. An integrated approach between international, supranational, and domestic sources of law would not be sufficient if not accompanied by other supplementary measures to be adopted in a systemic perspective, including resorting to the combined use of disciplines born to regulate different areas, as, for example, already happens with antitrust regulation. Said disciplines, despite their specificity, can, in turn, bring very valuable protection in contexts that are insufficiently manned or in which the boundaries between what is market regulation and what is a guarantee for the fundamental rights of the person tend to blur a great deal.

Big Tech are often the drivers of technological innovation; they exploit technological innovation to maintain a leading role even in the protection of fundamental rights, effectively evading any attempt at regulation. This aspect, which is often little considered, is actually crucial because a prompt response to change, in regulatory terms, cannot be achieved without the utmost knowledge and understanding of the technological sphere; rights in the digital world can only be protected by technology and a specialized knowledge of it.

Legislators and regulators should not only stay abreast of technological advances, but actively participate in them, focusing on the development of law disciplines within a technological paradigm. An excellent example of such a kind of integration is again the GDPR of the European Union, which establishes clear rules on the management of personal data, but also requires an understanding of the technical aspects to ensure their processing is compliant.

1.2. The Challenge of Biometrics

As already pointed out at the beginning of the discussion, a more integrated approach between regulatory sources and information technology is desirable to reduce legislative response times and address new challenges that technology brings to the regulatory field in a timely manner. This approach would allow for the rapid identification of relevant technologies that influence the secure use of technology in the short term; one of these is certainly biometrics, especially considering that biometric data is already present in European eID cards.

The use of biometric data can be a key element in addressing new challenges emerging in various areas, such as security, personal identification, and access to digital services. However, the widespread adoption of biometric data is still held back by issues of privacy, security, and balancing individual and collective rights. The collection and use of biometric data raises legitimate concerns [10–12] about protecting people's privacy, access to and control over their personal data, and the possibility of abuse or security breaches. Computer science can contribute by developing secure methods for collecting, processing, and storing biometric data; the application of machine learning and artificial intelligence algorithms can help improve the accuracy and reliability of biometric systems. However, how can this be done in an appropriate regulatory framework?

1.3. Related Work and Outline of the Paper

To adequately address these concerns and fully contextualize the contribution of this work within the broader landscape of digital identity research, three main aspects need to be considered. First, we need to consider decentralized biometric techniques, i.e., those that can be efficiently implemented on common mobile devices without requiring specialized hardware or sensors. This area of research has been promoted in recent years by the advent of deep learning techniques, which have far surpassed previous holistic and geometric approaches [13]. Secondly, the schemes underlying biometric authentication must be analyzed. This has to do with how an external Identity Provider connects to the mobile device and how biometric data is collected and manipulated [14]. Finally, the problem of preserving privacy through a balanced approach that considers both the protection of sensitive personal data and collective needs while ensuring an adequate level of security is fundamental.

Building on this premise, the paper first undertakes an analysis of the emerging notion of digital identity, highlighting how technological progress has shaped its evolutionary path. Particular attention is given to the role of digital identity in accessing network resources and/or conducting digital transactions.

This aspect is explored in Section 2, where some basic authentication schemes are illustrated, and the complexities associated with the introduction of biometric authentication are briefly outlined in full compliance with current regulations. Section 3 looks at European regulation and, more specifically, at the challenges related to interoperability among EU Member States in the implementation of the eIDAS Regulation. Section 4 proposes a new authentication scheme based on existing biometrics and ID cards, but implementing a high level of security specifically designed for the most demanding applications. This solution, if implemented, could be an opportunity for the European identification system to easily adopt and extend this technology to the whole European area. Section 5 discusses the benefits and concerns of the proposed method, addressing both technological aspects and potential regulatory impacts. Finally, Section 6 presents the conclusions and offers final remarks.

2. From Personal Identity to Digital Identity

With the rise of the Digital Society, the legal framework of privacy regulation is being enriched with a new notion, "digital identity", which has now become part of the vocabulary of jurists and legislators around the world.

Commonly, it is declined in two distinct ways; according to the first and broader meaning, the expression is used as a synonym for "networked" or "virtual" identity. Frequent is its use within the legal and sociological debate [15] regarding the possibility of "fake identities" online [16] (e.g., names and personal information different from those used in real life) or the use of "vague identities" (pseudonyms or nicknames).

On the contrary, according to a narrower meaning, typically attributable to specialists in computer law, the expression digital identity is defined as "the set of information and resources granted by a computer system to a particular user of said system" [17]. Obviously, said information is usually protected by an authentication system based on passwords,

additional devices (magnetic card, smart card, etc.), or biological traits (iris, fingerprint, face, etc.).

The latter meaning of digital identity is commonly referred to in the now substantial literature on the subject of "identity theft" [18]; in fact, it already emerges clearly how any discourse on digital identity must necessarily touch two aspects, namely the protection of personal identity on the Web, which we have already argued about previously, and the techniques of subject authentication by means of computer tools, which we will discuss next.

To better explain this aspect, we start by noting that the terms "authentication" or "identity verification" generically refer to the process needed to ascertain the identity of an individual, both physically (for example, in the case of an airport police checkpoint) or remotely; in the latter case, when the process is essentially automated by computer tools, the terms "electronic identification" (eID) is commonly adopted.

It is also worth noting that personal data (which define personal identity) can include a very diverse range of information: these data can uniquely distinguish a person in business practices (e.g., name, date and city of birth, identification number, social security code) or be part of a more intimate set of personal traits that uniquely represent a human being (e.g., fingerprints, iris prints, photographs) or that relate to his or her cultural or social identity (e.g., gender, ethnic group, nationality, religion). Not all these data are significant for transactions, nor to ascertain the identity of the individual; moreover, not all these data must be necessarily stored on a computer or be part of a computer representation.

What matters, in this perspective, is the viability of a technological solution for reliably establishing the identity of a natural or legal person in the context of a digital transaction through an electronic identification process that we will also better denote as a "digital identity scheme for the transaction" [19]. Please refer to the next section for a more detailed discussion of this concept.

Digital Identity Schemes for Transactions

Electronic identification is the gateway to many public and private services; among these, it is strictly required for private services (bank accounts, insurance, car rental, hotel booking), government services (certificates, taxes, driving license), education (enrollment, exams), and access to medical treatments or data. However, note that rarely do these services rely on a common digital identity scheme. Most of the time, public providers act like commercial providers (e.g., social media or shopping online), issuing credentials, adopting proprietary access schemes, and storing data independently [20]. This attitude has been recognized as the main cause of an exponential increase in account numbers and privacy breaches.

As illustrated in Figure 1, actual digital identity schemes are based on two distinct phases:

1. An enrollment phase which must precede the identification process in order to release personal credentials. During this phase, a person appears before a civil registry office that verifies the personal identity and acquires the additional personal information necessary to fully define the digital identity. Commonly, all of this information (personal data) is stored within an electronic medium (e.g., a microchip ID card) and/or in a protected database. The tangible and/or intangible element containing the personal information used for online service authentication is also known as "electronic identification mean". Because some personal information may change over time, the literature often views enrollment as an ongoing process, with regular updates that must be applied five to ten years apart.
2. Once the digital identity of a person has been defined through the enrollment phase, such a person can undergo electronic identification (eID) and gain access to IT resources and services.

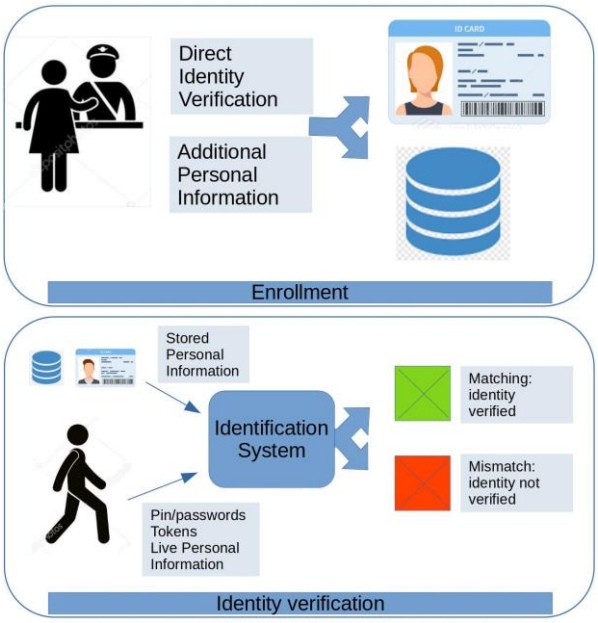

Figure 1. The two phases of a digital identity scheme.

Note that a recent trend in Europe, led by the evolution of smartphones and more convenient for users, is the adoption of mobile-based solutions for performing electronic verification.

More precisely, the system involves the following main entities and components:

- The user who wants to access an online service through his mobile device;
- The browser or other application used by the user to access online services;
- The IdP that manages the authentication procedure;
- The SP which, after requesting user authentication from the IdP, manages the authorization and delivers the requested service;
- The ID App, a mobile application provided by the IdP, needed to challenge the credentials of the user;
- The ID card, which is one of the possible authentication means (containing personal data) involved in the scheme;
- To enhance security, the ID App often employs "secure" multi-factor authentication, combining elements such as something the user knows (e.g., a password or PIN) and something the user owns (e.g., a token generator or a card); a further evolution of these systems is the use of embedded biometric authenticators that mostly include biometric sensors for fingerprint or face recognition. This solution is often used in place of the PIN code since it is considerably more user-friendly but brings a lot of security concerns, as better described in Section 3.3.

In summary, the definition of digital identity schemes poses a complex challenge to the legal discipline and requires adequate integration of information technology, as it involves the management and protection of sensitive personal data. Existing schemes already provide a fair level of security, but they intentionally avoid biometric recognition precisely because of the sensitivity of biometric data. Moreover, there is a problem of interoperability and data management of a supranational nature that necessarily needs to be addressed to pave the way for a broader field of application. The following section illustrates how this could be done, at least in the European sphere, without excessive disruption.

3. European Electronic Authentication Regulation

The EU does already have a regulation on electronic authentication systems (eIDAS—Regulation EU No. 910/2014 on digital identity), which was issued in 2014 but has been effective since 2016 [21]. The eIDAS (electronic IDentification Authentication and Signature)

is a European framework that permits secure authentication with national credentials when accessing online services in any Member State (MS). The aim is to create a standard normative framework for trusted and secure online interactions between individuals, enterprises, and government agencies, as well as to improve the efficiency and security of online services and transactions within the European Union. The MS who wants to adhere to eIDAS must notify electronic identification (eID) schemes to the European Commission. Furthermore, if a MS wants to grant access to an online public service through an eID scheme, then it must also accept the notified schemes of other countries. The national eID schemes are interoperable thanks to the eIDAS Solution, which consists of a protocol designed to convert national identification data into a standard format that MSs can understand and use, as depicted in Figure 2.

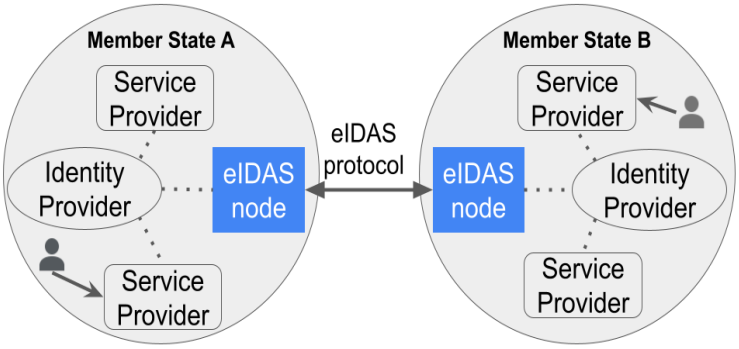

Figure 2. High-level overview of the eIDAS solution.

Under the eIDAS Regulation, eID schemes are classified according to three Levels of Assurance (LoA) corresponding to the degree of trust in a person's claimed identity during an electronic identification. This parameter is useful to compare identification procedures and authentication methods, based on security, robustness, and issuance process. The three LoA levels are the following:

(a) Low (L)—refers to identification means that ensure a limited security level regarding the declared identity of a person; it comprises procedures and technical methods to reduce the risk of violation or counterfeit of the identity; for example, the one-factor, which uses username a password belongs to this level.

(b) Substantial (S)—refers to identification means that ensure a substantial security level regarding the claimed or declared identity of a person; it comprises procedures and technical methods to effectively reduce the risk of abuse or counterfeit of the identity; for example, two-factor authentication belongs to this level, which uses username–password combined with a one-time password (OTP).

(c) High (H)—refers to identification means that ensure a higher security level regarding the claimed or declared identity of a person than the means used at the substantial level; it comprises procedures and technical methods to avoid the risk of abuse or counterfeit of the identity; an example is two-factor authentication combined with a secure device, which uses credentials, and public–key authentication based on a chip.

In 2023, 22 MSs have notified 28 eID schemes under eIDAS (as reported in Table 1).

Table 1. Electronic identification schema notified by Member States under eIDAS framework.

Title of the Scheme	eID Means	Member State	LoA	Year
German eID based on Extended AccessControl	National Identity Card, Electronic Residence Permit	Germany	H	2017
SPID—Public System of Digital Identity	SPID eID means provided by private providers	Italy	H-S-L	2018
Italian National ID card (CIE)	Carta di Identità Elettronica (CIE)		H	2019

Table 1. *Cont.*

Title of the Scheme	eID Means	Member State	LoA	Year
Belgian eID scheme FAS/eCards	Belgian Citizen eCard; Foreigner eCard	Belgium	H	2018
Belgian eID scheme FAS/Itsme	itsme mobile App		H	2019
Estonian ID card	ID card	Estonia	H	2018
Estonian RP card	RP card		H	2018
Estonian Digi-ID	Digi-ID		H	2018
Estonia e-Residency Digi-ID	e-Residency Digi-ID		H	2018
Estonian Mobiil-ID	Mobiil-ID		H	2018
Estonian diplomatic ID card	Diplomatic ID card		H	2018
Documento Nacional de Identidad electrónico (DNIe)	Spanish ID card (DNIe)	Spain	H	2018
Luxembourg national identity card (eID card)	eID card	Luxembourg	H	2018
National Identification and Authentication System (NIAS)	Personal Identity Card (eOI)	Croatia	H	2018
Cartão de Cidadão (CC)	eID card	Portugal	H	2019
Chave Móvel Digital	Digital Mobile Key		H	2020
National identification scheme	Czech eID card	Czech Republic	H	2019
Dutch Trust Framework for Electronic Identification	Means issued under eHerkenning (for businesses)	The Netherlands	H-S	2019
DigiD	DigiD Substantieel, DigiD Hoog		H-S	2020
Latvian eID scheme (eID)	ID Karte; eParaksts karte; eParaksts	Latvia	H-S	2019
National identity scheme	Slovak Citizen eCard, Foreigner eCard	Slovakia	H-S	2019
Lithuanian National Identity	Lithuanian National Identity card (eID/ATK)	Lithuania	H	2020
NemID	ey card (OTP); Mobile app; Key token (OTP); NemID hardware; Interactive Voice/Response (OTP); Magna key card (OTP)	Denmark	S	2020
Swedish eID	BankID; Freja eID (Notified); EFOS	Sweden	H-S	2020
French eID scheme 'FranceConnect+' 'The Digital Identity La Poste'	-	France	S	2021
Identity Malta	Maltese eID card and e-residence documents	Malta	H	2021
Norwegian eID scheme Buypass ID	Buypass ID	Norway	H	2021
ID Austria	-	Austria	H	2022
Public Electronic Identification System	Trusted profile, personal profile	Poland	H-S	2023
eID.li, Class A	-	Liechtenstein	H-S	2023
Slovenian eID card scheme	SI eID card	Slovenia	-	2023

3.1. Interoperability among EU Member States

As of 2018, a Member State that offers access to a public online service through an eID scheme is obliged by the eIDAS Regulation to accept notified eIDs from other member states. This concerns online services related to a "substantial" or "high" LoA. However, the regulation's goal of being technology-neutral has resulted in a variety of interpretations of the obligations among MSs and in a high heterogeneity of implementations, giving rise to difficult interoperability.

Some MSs have more than one eID scheme, and in many cases, within the same scheme different means can be used (according to the correspondent LoA). For example, some

of the schemes notified by MSs rely on the chip of the national eID cards. This approach corresponds to the higher LoA and exploits eID cards with broad population coverage, enforcing strong identity proofing. However, only 14 out of 28 schemes exploit the national ID card. The observation is important because it highlights the diversity and challenges in achieving interoperability among EU Member States' eID schemes. It underscores the need for ongoing efforts to harmonize eID implementations, enhance security and user convenience, and support the overarching objectives of the eIDAS Regulation for a more integrated digital single market. A step in this direction is marked by Regulation (EU) 2019/1157, which mandates that ID cards are harmonized across the EEA, with a new common identity card model replacing the various formats. This harmonization, along with the progressive adoption of the eIDAS Regulation by Member States, will allow for the maximum scalability of the proposed solution across Europe.

According to Table 1, MSs and Identity Providers are increasingly shifting away from traditional card-based eID schemes, which require card readers, toward mobile-based solutions, which are more practical for end users. The most recent schemes, where more eID means involve smartphones, clearly show this trend. For greater security against attacks, these eID methods can make use of software programs as well as hardware-embedded elements like SIM cards, Secure Element, and Trusted Execution Environment. However, technology and the specific mobile phone being utilized have a significant impact on how secure such an embedded device is.

3.2. eIDAS Regulation Revision

Since the COVID-19 pandemic has had a significant impact on digitalization speed, both governmental and commercial sector services are becoming increasingly digitized, and citizens and businesses are expecting high security and convenience when doing online transactions (such as paying taxes, asking for a loan or opening a bank account from a distance, starting a business in another MS, buying online). Thus, today, users are becoming more demanding regarding online public and private services. For example, they are expecting seamless online journeys, mobile applications, and single-sign-on solutions. However, the eIDAS framework was conceived targeting secure cross-border access to public services, which is a limited portion of individuals' and enterprises' electronic identification needs. A recent evaluation of the framework revealed that the existing regulation does not adequately address several issues regarding user expectations and market demands, which results in a limited uptake among European citizens and companies [22]. The report shows that the services addressed primarily concern the 3% of the EU population who live in a MS other than their birthplace. Additionally, the existing eIDAS architecture prevents users from facilitating the GDPR principles of data minimization and privacy by default by deciding what data to share and with whom. According to the report, only 14% of public service providers offer authentication via eIDAS.

The European Commission identified the lack of awareness and understanding of the regulation as one of the main blocking factors for the uptake of eID from service providers. Simultaneously, the poor user experience is discouraging them from entering the eIDAS Network since it is perceived as a risk of compromising the quality of the services they provide. Moreover, two main roadblocks to the long-term maturation of the legal framework are the absence of a business model for private Identity Providers and the vagueness of the terms and conditions of access to the eIDAS network for private relying parties.

The report's conclusion is that the current eIDAS Regulation, with its built-in restrictions on the public sector, the difficulty for online private providers to connect to the system, its inadequate availability in all MSs, and its lack of adaptability to support a range of cases, cannot meet these new market demands. To meet new policy objectives, user expectations, and market demand while also considering recent breakthroughs in digitalization, the eIDAS Regulation must be upgraded in terms of effectiveness, efficiency, coherence, and relevance.

3.3. Weaknesses and Limits of the eID Scheme

The use of biometric data in the context of eIDAS implies strict compliance with data protection regulations, including the General Data Protection Regulation (GDPR). The challenge lies in the fact that eIDAS acknowledges the presence of biometric data but does not impose mandatory requirements. Instead, it provides a legal framework for use, leaving the decision to use biometric data in eID services up to EU Member States and the organizations implementing these services. Consequently, the misuse of digital identities persists because biometric data in eIDs are not uniformly used, and there is no guarantee that the person accessing a digital identity is indeed its rightful owner.

Although almost all countries use at least one eID scheme with a high level of security, it is not comprehensive enough to defend the user's identity. This is also confirmed by the analysis of levels of security of the different eID schemes in eIDAS provided by [23] leveraging the MuFASA tool by NIST. Concerning the use of biometrics, none of the eID schemes adopted today include biometric authentication, but some of them allow the use of biometric authenticators embedded in smartphones and provided by the operating system. This authentication modality allows bypassing the input of username and password, improving the usability of the application but also raising paramount security concerns. First, the biometric data registered in the device could belong to a different person than the cardholder, i.e., the keys can be associated with the biometric data of a different person who can use it to bypass the 1-factor authentication step. Furthermore, current mobile phones allow registering more than one biometric, which can be used to verify the identity of the user interchangeably; it is thus possible to register more fingerprints belonging to different fingers and to acquire facial information, even from different users. These biometric accesses are not associated with the specific user who generated them but with the mobile devices where they are stored. It is thus possible that two different persons can access the same device with two different biometric data (e.g., one with the fingerprint and the other with the face recognition). This is a realistic scenario for shared devices, for example with relatives, like wives with husbands, father/mother with son/daughter, etc.

4. Biometric Identification as a Unique Opportunity

Although biometric authentication technologies are not a recent topic [24–26], the widespread use of smartphones opened new development and commercial opportunities for these solutions. It has been foreseen by [27] that by 2022, more than 5.5 billion mobile devices will be used to verify, through biometric authentication, 1.37 trillion transactions. Thanks to the evolution of integrated devices like HD and depth cameras and LIDAR (LIght Detection And Ranging is a laser system that allows measuring the distance between a surface and the laser source, measuring the time for the reflected light to return to the receiver) and faster network speeds, the opportunity for commercial innovation has led to the development of new biometric identity verification solutions that are more secure and with improved customer experience.

Commercial identity verification providers have been able to produce applications that read data from the chip inside electronic identity documents thanks to the constant expansion of smartphone functionality, particularly features in devices that use Near Field Communication (NFC). Reading the identifying features directly from the chip, including the digital image of the document's owner's face, drops the risk of photo substitution forgery and improves data capture accuracy [28].

In the following, an innovative authentication scheme exploiting mobile phones, eID cards, and face recognition is proposed. A possible implementation is illustrated in Figure 3, where the current eID card-based authentication schema is integrated with biometric data. The authentication procedure begins when the user accesses the SP's website using a standard browser on a mobile or desktop device (steps 1–2). During the login phase, a query is redirected to the IdP, which requests biometric authentication via the ID APP (step 3). The ID APP exchanges data with the Identity Provider to confirm the user's identity (steps 4–5). The ID APP retrieves the gallery (step 6b) and probe data (step 6c)

and matches them to verify the user's identity. If the match is successful, the IdP grants authentication (step 7), and the ID APP reopens the browser (step 8) to contact the SP, allowing the user to access the service. Further details on the implementation of this solution are provided in Sections 4.2 and 4.3, as well as in Figures 4 and 5.

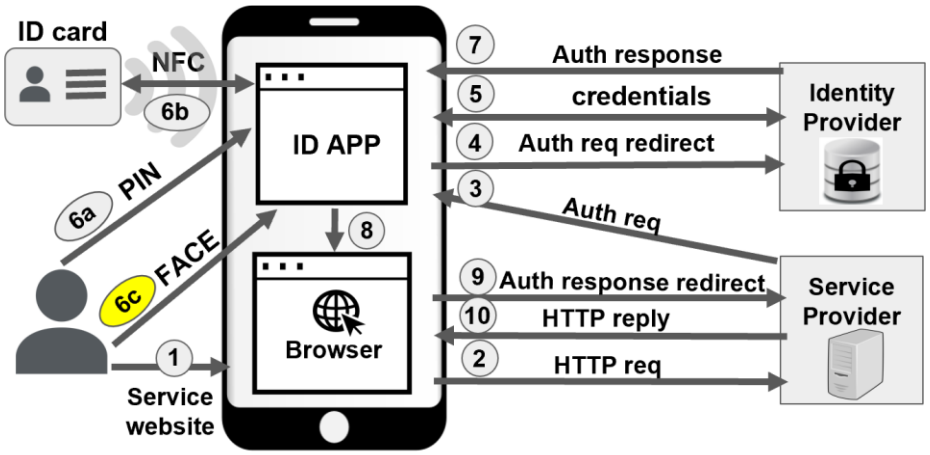

Figure 3. Integration of the face recognition task in the current eID authentication schema.

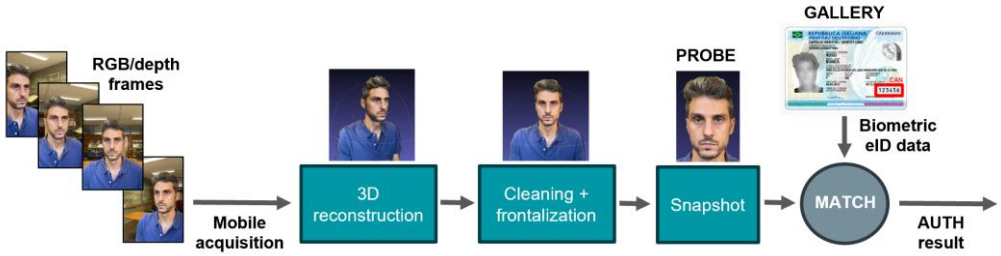

Figure 4. Schema of the process of generating the probe and gallery images for the face recognition algorithm.

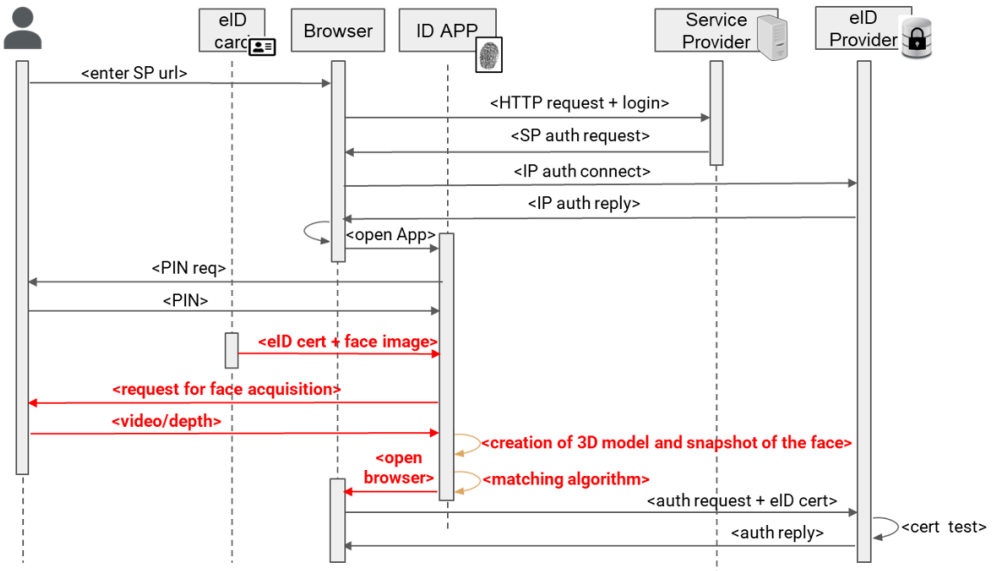

Figure 5. Authentication scheme of the proposed solution integrated within a simplified version of the eID's authentication scheme.

4.1. Italian eID Card (CIE)

The CIE (Italian electronic identity card) version 3.0 is already distributed in more than 90% of the Italian territory, with about 27.5 million cards issued in 2022 [29]. This electronic card allows the secure identification of the holder through the verification of personal and biometric data stored inside the microchip and protected according to the same security mechanisms used for passports and residence permits (thus compliant with the same control systems applied for border crossings). The personal and biometric data of the holder (headshot and fingerprints), as well as the information that allows for online identification, are securely stored inside the CIE's microchip. An overview of the authentication process is shown in Figure 2. The main functions of the CIE are provided by two applications implemented in the chip: (i) identity verification, provided by the Machine-Readable Travel Document application (MRTD); (ii) access to online services, provided by the IAS ECC application. The information contained in the CIE is accessible in different ways and according to different levels of protection, as described in Table 2.

Table 2. The data included in the national electronic ID card (eID) and the related access mode can be illustrated using the example of the Italian CIE.

Access Mode	Data
Freely	- unique card identifier (NIS) - name and surname - date and place of birth - gender and nationality
Scanning the MRZ code or by typing the CAN number (both printed on the card)	- validity for traveling abroad - picture of the face - parents (if the card was emitted when the owner was not of legal age) - address (when the card was emitted) - tax code and ID number
Typing the PIN (provided separately)	- TLS client certificate
Only by law enforcement	- fingerprints

4.2. Digital Identity Verification with eID Card's Biometric Data

The image of the face stored in the eID card's chip (referred to here as gallery image) is freely accessible and can be easily retrieved with a specific API. Different mobile applications that can read the NFC chip and retrieve this data can be freely downloaded from the app stores. A very effective method for verifying if a person is the real owner of the digital identity is to compare the gallery image with a photo taken during the authentication with the camera of the mobile device (referred to here as probing image). It could be argued that with modern technologies, like hyper-trained AI algorithms, a 1:1 verification is a relatively easy task to accomplish. Unfortunately, it is not always the case. As reported by the NIST in its Facial Recognition Vendor Test (FRVT) [30], facial recognition systems can achieve near-perfect accuracy under ideal conditions, reaching accuracy scores as high as 99.9999%. The ideal conditions with regard to face images (such as passport photos or mugshots) are defined by the ISO Standard for Biometric Data Interchange [31], which require consistency in lighting and head pose as well as clear and unobscured facial features of the subject. Also, eID cards are compliant with this standard and contain a very clear picture of the face, taken by an operator in a controlled environment (without noise in the background and with full direct light) with specific recommendations (do not cover the face, do not make facial expressions, etc.). The quality of the picture is at the end of the process ensured by the operator. Moreover, the data are stored within the secure element of the eID card in accordance with standard security measures, such as those defined by ICAO 9303 and Regulation (EU) 2019/1157 of the European Parliament and of the Council. However, if images taken in the real world with commercial devices are used, facial recognition systems have a degree of accuracy far lower. The quality of the probing image acquired with the

mobile device is extremely dependent on the precision of the camera. Furthermore, the acquisition takes place in uncontrolled environments, with noisy backgrounds, variable light conditions or shadows, and uncontrolled subjects who may not be looking directly at the camera. These conditions are often called "in the wild". According to the FRVT [30], the incorrect rejection rate of the leading matching algorithms goes from 0.0001% when using VISA photos to 0.27% when using pictures of faces captured "in the wild", resulting in systems with less usability.

In the following section we propose a novel solution to improve the performance of a facial recognition system, exploiting the eID's biometric data. More details about the implemented solution can be found at [32]. The solution envisages 3D reconstruction technologies, such as monocular reconstruction and depth sensor scans, to create a 3D model of the user's head; such a model, cleaned of environmental noises (light conditions, background, others), can be used to generate a frontal snapshot of the face, to be compared with the CIE's image. A schema outlining the authentication pipeline is depicted in Figure 4. The probe image is generated as a snapshot of the user's 3D facial model, while the gallery image is retrieved from the eID card using NFC technology. Both images are then processed through a machine learning face recognition algorithm to obtain the final authentication result.

4.3. Enhancing Biometric Verification with 3D

As discussed above, the main issue with the use of real-world images as probing images is that, individually, they cannot guarantee a sufficient level of accuracy in the verification process. However, rapid progress has been made recently in the field of 3D face reconstruction [33,34], with the development of novel and powerful algorithms, faster, more accurate, and energy efficient [35], which can obtain impressive results even in the challenging case of reconstruction from a single RGB camera [36,37]. These techniques are extensively used in forensic applications, particularly for face-based identification, where 3D model reconstruction overcomes the shortcomings of 2D images acquired in crime scenes [38].

The face's geometry is typically modeled as a set of triangles or quad meshes, to which added material properties describe the interaction of the skin with light. Modeling the light surface interactions for a face is an extraordinarily complex task; thus, in some cases, these complexities can be loosened using approximated appearance models with simple reflectance maps and illumination schemes. Furthermore, to allow the reconstruction of the face from images taken in the real world, i.e., in the ill-posed monocular setting, priors that simulate the shape and expression of faces are often used [39,40]. These priors are typically based on:

- Blend shape expression models (3D models of a particular fundamental expression);
- Parametric face models (low-dimensional face reconstruction from high-resolution laser scans of hundreds of human faces with neutral expressions).

The adoption of these priors not only solves the ill-posed problem but also enables reconstruction results of high quality, as proved by ZollHofer and colleagues [41].

The minimum requirement for the proposed method is to have a standard RGB camera to capture a short video of the face. This means that the method can be applied not only to mobile devices but also to laptops and desktop PCs equipped with a webcam.

Another way to reconstruct a 3D model of the face of a person is to use depth cameras. A depth camera is a device that is increasingly used in modern smartphones which can produce a map of distances between the illuminated surfaces and the camera. The measure of each point is based on the time-of-flight (ToF), i.e., the round-trip time of the signal produced by the sensor. Typically, laser or LED lights are used. Every brand produces its specific depth sensor. For example, Apple patented the TrueDepth camera [42], which consists of a traditional camera, an infrared camera, a proximity sensor, and a dot projector, as well as a flood illuminator. This sensor can project more than 30,000 dots, which enables

the creation of a dense model of the face. The sensor is used mainly for unlocking the smartphone through facial recognition but can also be used for photo editing.

Once the 3D model is created, it can be adjusted to correct skin reflectance and mitigate the sources of noise present at the time of the acquisition (poor light conditions, background, small occlusions). Moreover, the pose of the 3D reconstruction can be easily oriented to take a frontal snapshot of the face and use it as a probing image (as depicted in Figure 4). If a mobile device with a depth sensor is used, the 3D reconstruction will be more accurate and can be performed even under poor lighting conditions.

A possible implementation of this solution, integrated into the verification scheme of a national eID (for example, the Italian CIE), is depicted in Figure 5.

The eID authentication scheme is implemented through two distinct macro phases:

1. Request for the service displayed by the SP's portal/app, which takes place within the user's browser in the domain of the SP;
2. User authentication is performed directly by the IdP.

The request to access the eID authentication system takes place through a "call to action" made by the SP accessible through a special button. The button triggers the identification process through the IdP server component. This server performs the following functions:

- Performs digital identification of the user;
- Checks the validity of the certificate contained by the card;
- Displays the data that will be transmitted to the service provider;
- Sends an authentication assertion sealed with an Identity Provider-traceable seal to the service provider, which is proof of user recognition.

User authentication is initiated by the IdP, which requires activating the 3D acquisition and reading of the CIE data. A specific biometric ID app will allow 3D data to be acquired, the face model to be reconstructed, and the snapshot to be created before executing the verification algorithm (in red in Figure 5). The outcome of the verification will then be sent to the Identity Provider, who will reply to the Service Provider. The authenticity of the process and of the card used is verified by sending the X.509 digital authentication certificate present in the document chip and protected by the PIN code.

4.4. Empirical Validation

To validate the proposed method, it is essential to have a dataset comprising both 3D and 2D facial data of the subjects. Specifically, this dataset should include a controlled image of the subject (gallery), a 3D model of the face from which a clean, frontal snapshot can be extracted (probe for our method), as well as a selfie taken under uncontrolled conditions (probe for standard method). By comparing the gallery with the two different probes, using any facial recognition algorithm, it becomes possible to assess which input yields superior recognition results. From a literature review, two facial datasets have been identified that contain both required samples: the FRGC dataset from NIST [43] and the Bosphorus database provided by Philips Research and Boğaziçi University [44]. In our experiments, we used RetinaFace [45] to detect and crop the face and ArcFace [46] as the machine learning face recognition algorithm. The face images were then individually processed through the model to obtain face vectors, which could be compared using the cosine distance. A lower cosine distance indicates greater similarity between the two feature vectors, suggesting a higher likelihood that the two pictures are of the same face. This distance can be thresholded to form a binary classification decision of match or no match and calculate True Positive and False Negative statistics.

As shown in Table 3, which presents the results of the ROC curve analyses, the gain in using 3D data to build the probe images, as opposed to using uncontrolled data, is substantial. The table presents the values of the True Positive Rates (TPR) at two different False Acceptance Rates (FARs), demonstrating that, for the FRGC dataset, even under restrictive conditions (FAR = 10^{-6}), our method retains a good level of accuracy (76%), while the standard falls to values not acceptable for an authentication system (11%). The

advantage of using the 3D data with Bosphurus is not as evident as in the case of FRGC since the FAR = 10^{-6}; both methods reach nearly the same accuracy of 88%. The main reason for this is that the ambient illumination in the Bosphorus acquisitions is uniform across all expressions and poses, and the setting is constant (no background in any of the images). This means that the so-called "uncontrolled" images are, in fact, highly controlled in terms of illumination and background. In contrast, the uncontrolled images from the FRGC dataset exhibit more realistic characteristics. For a more extensive analysis of the validation of the proposed method, please refer to the paper [32], which provides detailed descriptions and results of a large number of experiments.

Table 3. Comparison of the performance of the proposed method (our) with standard 2D authentication methods (standard). Best values are highlighted in bold.

Dataset	Method	TPR@FAR = 10^{-3}	TPR@FAR = 10^{-6}	AUC
FRGC	our	**98.62**	**76.03**	**0.9997**
	standard	89.67	10.93	0.9842
Bosforus	our	**98.25**	**87.77**	**0.9992**
	standard	97.49	87.74	0.9983

5. Discussion

The method proposed in this paper, in addition to strengthening the verification's accuracy, introduces a set of improvements that will be briefly discussed in the following.

First, the usability is enhanced since it is no longer needed to remember complex codes or passwords to be prompted for the identification process. Some of the risks linked to the memorization of codes could be (i) forgetting them, which implies recovering them through an annoying procedure, and (ii) annotating them in a place where they can be stolen or accessed in a malicious way. Another relevant aspect regards the security of the system. In normal practice, centralized authentication servers are used to store biometric data. If these servers are compromised, the facial images of the users can be retrieved from the attackers. Another issue regards the liveness, i.e., the possibility that the user passes a photo retrieved online to fool the authentication system instead of taking one during the process [47]. The proposed method has a solution for both of these issues. First, the acquisition and the verification procedures are executed locally on the mobile device; thus, the sensitive biometric data (i.e., the probing images and the gallery images) are securely stored on the mobile device during the authentication procedure. After authentication, both the probe and gallery data are deleted and re-acquired with each authentication request. It is not necessary to exchange data through the network, unlike centralized systems. Moreover, the system includes intrinsic liveness detection since a video or a set of photos of the face needed to create the 3D model must be acquired live with the camera of the mobile phone. Finally, this method could be easily integrated into the standard identification scheme of CIE and does not require the use of special hardware (if the video reconstruction is used) making it compatible also with standard mobile devices.

Note that the proposed mobile authentication scheme involves creating a 3D model of the user's face, which is computationally demanding. Modern smartphones, often equipped with depth sensors and powerful CPUs, can handle complex tasks like 3D rendering and studies have shown that mobile devices can perform photorealistic 3D reconstruction in real time using depth sensors [48,49]. However, since not all devices have depth sensors, 3D monocular reconstruction could be necessary in some cases. Recent advances in deep learning have made this possible while maintaining accuracy and performance [50,51].

A final remark concerns some additional issues introduced by the proposed method; these are briefly discussed below.

- All manufacturers of mobile devices do not yet support NFC in all of their models;
- Each country could implement specific APIs since there are no universal guidelines for this development; consequently, different plugins would be required for each eID card to ensure the correct implementation of APIs for retrieving biometric data;
- Using a single biometric modality introduces weaknesses since it can be hacked or hijacked, even in scenarios where multi-factor authentication is implemented. A common practice recommends saving the evidence of the verification process (i.e., the probing image) for logging purposes. These data can cause problems with the storage capacity of the device;
- Modern attacks (like biometric spoof attacks, presentation attacks, video injection attacks, deep fake puppets, etc.) could compromise the system even in the presence of the liveness detection;
- If 3D monocular reconstruction is used, many parts of the reconstructed face model come from a generic template, which lacks person-specific idiosyncrasies and fine-scale skin details. Thus, the 3D face reconstruction techniques use simplifications and approximations which can result in slight changes of the face morphology.

As a further element of discussion, in Table 4, we present a qualitative comparison of some existing authentication approaches. Along with the description of each approach and the main drawbacks identified, the improvements achieved by using the method proposed in this work are highlighted.

Table 4. Comparison of the proposed method with existing authentication methods.

Method	Description	Drawbacks	Our Method
Username and password	The most common authentication method involves the use of secret codes known only to the user.	Codes must be memorized or recorded, which introduces the risk of them being forgotten, lost, or stolen. If the password is not strong enough, it can be easily guessed.	It is a passwordless method, thus eliminating the need for memorizing a secret. Users simply need to record a brief video of their face.
2D face recognition	This is the standard face recognition approach, utilizing one gallery image and one probe image.	When used with mobile devices, the probe images can be very noisy due to the uncontrolled acquisition process. The performance of face recognition algorithms significantly degrades with such images captured in uncontrolled environments.	Leverages 3D reconstruction to improve image quality by frontalizing the pose, enhancing contrast, improving illumination, and reducing noise, occlusions, and background elements.
3D face recognition	The data used for identity verification (both probe and gallery) are in 3D format.	The matching process is more computationally intensive, as the data must be aligned for accurate comparison. It is more challenging to find 3D datasets for training the algorithms.	Combines the benefits of both 3D and 2D methods. The 3D component allows for the adjustment and enhancement of image quality, while the 2D component leverages state-of-the-art face recognition systems, which perform exceptionally well with clean, high-quality images.

Table 4. *Cont.*

Method	Description	Drawbacks	Our Method
Traditional Biometric mobile authentication	This method enrolls the user the first time they use the app, then stores a gallery data on the device for subsequent authentications (e.g., Apple Face ID, Samsung Pass, etc.).	The user's real identity is not verified during the enrollment process. The actual matching between digital identity and real identity is not ensured. Additionally, if the device is shared with other users, multiple biometric gallery data can be stored. This means that any user with an account on the authentication system can potentially be authenticated.	The gallery data is retrieved from the eID card, which is issued by the national authority. During the enrollment phase, an operator verifies the identity of the individual and checks the quality of the data collected.
Centralized systems	This method involves a central repository, under full control of the provider, where credentials, whether traditional or biometric, are stored and retrieved for each authentication request.	The user loses control of their data, and the central repository becomes a single point of failure. If the repository is attacked, a large number of identities can be stolen. Additionally, data (probe image or gallery) must be transferred over the internet each time an authentication is requested.	The data are processed locally, and after authentication, both the gallery and probe data can be deleted from the device. This ensures that data are never shared or moved from the user's device.
Special HW	This method entails the use of specialized hardware to authenticate the user, such as a card reader or a code generator (OTP). These devices are typically used to enhance the modalities for authentication.	You need to carry specialized hardware with you. If you lose it or forget to bring it, you will not be able to authenticate.	This method adheres to the Bring Your Own Device (BYOD) approach. The system can run on a personal mobile device and can be used without the need for any additional specialized hardware.

6. Conclusions

The paper addresses the issue of digital identity, a concept of paramount importance in promoting automated access to network services and resources, while complying with European regulations and privacy requirements. The eIDAS Regulation, although in its early stages, establishes an important framework for all MSs. In addition, the technical solutions adopted by participating MSs show an interesting convergence toward the adoption of mobile devices and national eID cards based on advanced microchips capable of storing and protecting both transactional identity and additional personal information. On the other hand, some interoperability issues are emerging and, with this, the clear inadequacy of some of the proposed technical solutions. Meeting the adoption and requirements of end users for online authentication, more and more MSs have recently implemented solutions based on mobile devices. Among the limitations of current implementations is a lack of awareness and understanding of the regulation and poor user experience, particularly in the verification process. In order to overcome these limitations, the paper proposes a new identification paradigm based on existing biometric data and ID cards. It implements state-of-the-art 3D monocular reconstruction techniques through the use of highly popular and commonly used devices in the community (smartphones). This approach can ensure, in the short term, a very efficient verification process and a high level of security, which is typical for the most demanding applications such as those developed in healthcare or finance. In addition, the use of widely available and consolidated tools such as smartphones, which have become an integral part of our daily lives and offer a wide range of features and applications that simplify many of our activities, would increase awareness of the use of

the tool and the perceived trustworthiness of users, including against new identification and authentication solutions.

Although the eIDAS network is increasingly accepted by MSs, its integration with actual operational services is still at an early stage, and significant efforts are needed to extend and push the eIDAS framework as a common goal of the EU economy. Fortunately, many MSs have planned projects to implement e-government solutions, including the European digital identity, in their national plans under the Recovery and Resilience Instrument. If properly conducted, with an EU-wide perspective and gradual convergence of IT platforms, these projects could provide an incredible opportunity for the consolidation of the European economic space and renewed momentum toward the goal of full European citizenship.

The integration of regulatory and IT sources, in particular by leveraging biometric data, can offer significant advantages in addressing new legal challenges. The biometric solution proposed in this model ensures full compliance with GDPR and eIDAS regulations, and furthermore, implementing a robust security protocol allows for improved identity verification processes, guaranteeing the authenticity and security of individuals' identities and indirectly reinforcing legal frameworks.

Author Contributions: Conceptualization, P.R. and E.G.; Formal analysis, P.R., S.S. and E.G.; Funding acquisition, P.R. and E.G.; Investigation, P.R., S.S. and E.G.; Methodology, P.R., S.S. and E.G.; Project administration, P.R. and E.G.; Supervision, P.R. and E.G.; Writing—original draft, P.R., S.S. and E.G.; Writing—review and editing, P.R., S.S. and E.G. All authors have read and agreed to the published version of the manuscript.

Funding: This work received financial support under the National Recovery and Resilience Plan (NRRP), Mission 4, Component 2, Investment 1.1, Call for tender No. 1409 published on 14 September 2022 by the Italian Ministry of University and Research (MUR), funded by the European Union—NextGenerationEU—Project Title "METATwin—Metaverse & Human Digital Twin: digital identity, Biometrics and Privacy in the future virtual worlds",—CUP J53D23015030001—Grant Assignment Decree No. 0001382 adopted on 1 September 2023 by the Italian Ministry of University and Research (MUR). Moreover, this work has been developed within the framework of the project e.INS-Ecosystem of Innovation for Next Generation Sardinia (cod. ECS 00000038) funded by the Italian Ministry for Research and Education (MUR) under the National Recovery and Resilience Plan (NRRP)—MISSION 4 COMPONENT 2, "From research to business" INVESTMENT 1.5, "Creation and strengthening of Ecosystems of innovation" and construction of "Territorial R&D Leaders".

Data Availability Statement: For this work, no new data were created.

Conflicts of Interest: The authors declare no conflicts of interest. The funders had no role in the design of the study, in the collection, analyses, or interpretation of data, in the writing of the manuscript, or in the decision to publish the results.

References

1. Solove, D.J. *The Digital Person: Technology and Privacy in the Information Age*; NyU Press: New York, NY, USA, 2004; Volume 1.
2. Janssen, M.; Helbig, N. Innovating and changing the policy-cycle: Policy-makers be prepared! *Gov. Inf. Q.* **2018**, *35*, S99–S105. [CrossRef]
3. Wright, D.; Gutwirth, S.; Friedewald, M.; De Hert, P.; Langheinrich, M.; Moscibroda, A. Privacy, trust and policy-making: Challenges and responses. *Comput. Law Secur. Rev.* **2009**, *25*, 69–83. [CrossRef]
4. Rule, J.B.; Greenleaf, G.W. (Eds.) *Global Privacy Protection: The First Generation*; Edward Elgar Publishing: Cheltenham, UK, 2010.
5. Casagran, C.B. *Global Data Protection in the Field of Law Enforcement: An EU Perspective*; Routledge: London, UK, 2016.
6. Regulation, P. Regulation (EU) 2016/679 of the European Parliament and of the Council. *Regulation (EU)* **2016**, *679*, 2016.
7. Data, P.O.P. Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Off. J. L* **1995**, *281*, 0031–0050.
8. de Terwangne, C. Council of Europe convention 108+: A modernised international treaty for the protection of personal data. *Comput. Law Secur. Rev.* **2021**, *40*, 105497. [CrossRef]
9. Bellanova, R.; Carrapico, H.; Duez, D. Digital/sovereignty and European security integration: An introduction. *Eur. Secur.* **2022**, *31*, 337–355. [CrossRef]
10. Prabhakar, S.; Pankanti, S.; Jain, A.K. Biometric recognition: Security and privacy concerns. *IEEE Secur. Priv.* **2003**, *1*, 33–42. [CrossRef]

11. Payton, T.; Claypoole, T. *Privacy in the Age of Big Data: Recognizing Threats, Defending Your Rights, and Protecting Your Family*; Rowman & Littlefield: Lanham, MD, USA, 2023.
12. Romanou, A. The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise. *Comput. Law Secur. Rev.* **2018**, *34*, 99–110. [CrossRef]
13. Ríos-Sánchez, B.; Silva, D.C.-D.; Martín-Yuste, N.; Sánchez-Ávila, C. Deep learning for face recognition on mobile devices. *IET Biom.* **2020**, *9*, 109–117. [CrossRef]
14. Ekpezu, A.O.; Umoh, E.E.; Koranteng, F.N.; Abandoh-Sam, J.A. Biometric Authentication Schemes and Methods on Mobile Devices: A Systematic Review. In *Modern Theories and Practices for Cyber Ethics and Security Compliance*; Yaokumah, W., Rajarajan, M., Abdulai, J., Wiafe, I., Katsriku, F., Eds.; IGI Global: Hershey, PA, USA, 2020; pp. 172–192. [CrossRef]
15. Nagy, P.; Koles, B. The digital transformation of human identity: Towards a conceptual model of virtual identity in virtual worlds. *Convergence* **2014**, *20*, 276–292. [CrossRef]
16. Vaast, E. Playing with Masks: Fragmentation and Continuity in the Presentation of Self in an Occupational Online Forum. *Inf. Technol. People* **2007**, *20*, 334–351. [CrossRef]
17. Flick, C. Falsa identità su Internet e tutela penale della fede pubblica degli utenti e della persona. *Il Diritto Dell'Informazione e Dell'Informatica* **2008**, *526*, 4–5.
18. Marshall, A.M.; Tompsett, B.C. Identity theft in an online world. *Comput. Law Secur. Rev.* **2005**, *21*, 128–137. [CrossRef]
19. Sullivan, C. Digital identity–From emergent legal concept to new reality. *Comput. Law Secur. Rev.* **2018**, *34*, 723–731. [CrossRef]
20. Sciarretta, G.; Carbone, R.; Ranise, S.; Armando, A. Anatomy of the facebook solution for mobile single sign-on: Security assessment and improvements. *Comput. Secur.* **2017**, *71*, 71–86. [CrossRef]
21. Council of European Union. Council Regulation (EU) no 910/2014. 2014. Available online: http://data.europa.eu/eli/reg/2014/910/oj (accessed on 23 June 2024).
22. Council of European Union. Report from the Commission to the European Parliament and the Council on the Evaluation of Regulation (eu) no 910/2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (Eidas). 2021. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021DC0290 (accessed on 7 June 2024).
23. Sharif, A.; Ranzi, M.; Carbone, R.; Sciarretta, G.; Marino, F.A.; Ranise, S. The eIDAS Regulation: A Survey of Technological Trends for European Electronic Identity Schemes. *Appl. Sci.* **2022**, *12*, 12679. [CrossRef]
24. Kataria, A.N.; Adhyaru, D.M.; Sharma, A.K.; Zaveri, T.H. A survey of automated biometric authentication techniques. In Proceedings of the 2013 Nirma University International Conference on Engineering (NUiCONE), Ahmedabad, India, 28–30 November 2013; pp. 1–6.
25. Ruiu, P.; Caragnano, G.; Masala, G.L.; Grosso, E. Accessing cloud services through biometrics authentication. In Proceedings of the 2016 10th International Conference on Complex, Intelligent, and Software Intensive Systems (CISIS), Fukuoka, Japan, 6–8 July 2016; pp. 38–43. [CrossRef]
26. Masala, G.L.; Ruiu, P.; Grosso, E. *Biometric Authentication and Data Security in Cloud Computing*; Springer International Publishing: Cham, Switzerland, 2018; pp. 337–353. [CrossRef]
27. Nikolouzou, E.; Karkala, S.; Agrafiotis, I.; Gorniak, S. eIDAS compliant eID Solutions, Security Considerations and the Role of Enisa. 2020. Available online: https://www.enisa.europa.eu/publications/eidas-compliant-eid-solutions (accessed on 7 June 2024).
28. Abate, A.F.; Nappi, M.; Riccio, D.; Sabatino, G. 2d and 3d face recognition: A survey. *Pattern Recognit. Lett.* **2007**, *28*, 1885–1906. [CrossRef]
29. Italian Ministry of the Interior, Cie. Available online: https://www.cartaidentita.interno.gov.it/en/about- (accessed on 7 June 2024).
30. Grother, P.; Ngan, M.; Hanaoka, K. *Ongoing Face Recognition Vendor Test (Frvt) Part 1: Verification*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2022.
31. *ISO/IEC 19794-5:2005*; Information Technology—Biometric Data Interchange Formats—Part 5: Face Image Data. International Organization for Standardization: Geneva, Switzerland, 2016.
32. Ruiu, P.; Lagorio, A.; Cadoni, M.; Grosso, E. Enhancing eID card mobile-based authentication through 3D facial reconstruction. *J. Inf. Secur. Appl.* **2023**, *77*, 103577. [CrossRef]
33. Pietro, R.; Mascia, L.; Grosso, E. Saliency-Guided Point Cloud Compression for 3D Live Reconstruction. *Multimodal Technol. Interact.* **2024**, *8*, 36. [CrossRef]
34. Gecer, B.; Ploumpis, S.; Kotsia, I.; Zafeiriou, S. Ganfit: Generative adversarial network fitting for high fidelity 3d face reconstruction. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, Long Beach, CA, USA, 15–20 June 2019; pp. 1155–1164.
35. Nixon, S.; Ruiu, P.; Cadoni, M.; Lagorio, A.; Tistarelli, M. Exploiting Face Recognizability with Early Exit Vision Transformers. In Proceedings of the 2023 International Conference of the Biometrics Special Interest Group (BIOSIG), Darmstadt, Germany, 20–22 September 2023; pp. 1–7. [CrossRef]
36. Grassal, P.W.; Prinzler, M.; Leistner, T.; Rother, C.; Nießner, M.; Thies, J. Neural head avatars from monocular rgb videos. *arXiv* **2021**, arXiv:2112.01554.
37. Gafni, G.; Thies, J.; Zollhofer, M.; Nießner, M. Dynamic neural radiance fields for monocular 4d facial avatar reconstruction. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, Nashville, TN, USA, 20–25 June 2021; pp. 8649–8658.

38. Nixon, S.; Ruiu, P.; Trignano, C.; Tistarelli, M. Forensic Biometrics: Challenges, Innovation and Opportunities. In *Driving Forensic Innovation in the 21st Century: Crossing the Valley of Death*; Springer International Publishing: Cham, Switzerland, 2024; pp. 165–194.
39. Egger, B.; Smith, W.A.; Tewari, A.; Wuhrer, S.; Zollhoefer, M.; Beeler, T.; Bernard, F.; Bolkart, T.; Kortylewski, A.; Romdhani, S.; et al. 3d morphable face models—Past, present, and future. *ACM Trans. Graph. TOG* **2020**, *39*, 1–38. [CrossRef]
40. Blanz, V.; Vetter, T. A morphable model for the synthesis of 3d faces. In Proceedings of the 26th Annual Conference on Computer Graphics and Interactive Techniques, Los Angeles, CA, USA, 8–13 August 1999; pp. 187–194.
41. Zollhöfer, M.; Thies, J.; Garrido, P.; Bradley, D.; Beeler, T.; Pérez, P.; Stamminger, M.; Nießner, M.; Theobalt, C. State of the art on monocular 3d face reconstruction, tracking, and applications. In *Computer Graphics Forum*; Wiley Online Library: Hoboken, NJ, USA, 2018; pp. 523–550.
42. Breitbarth, A.; Schardt, T.; Kind, C.; Brinkmann, J.; Dittrich, P.G.; Notni, G. Measurement accuracy and dependence on external influences of the iphone x truedepth sensor. In Proceedings of the Photonics and Education in Measurement Science 2019, Jena, Germany, 17–19 September 2019; pp. 27–33.
43. Phillips, P.J.; Flynn, P.J.; Scruggs, T.; Bowyer, K.W.; Chang, J.; Hoffman, K.; Marques, J.; Min, J.; Worek, W. Overview of the face recognition grand challenge. In Proceedings of the 2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'05), San Diego, CA, USA, 20–25 June 2005; Volume 1, pp. 947–954.
44. Savran, A.; Alyüz, N.; Dibeklioğlu, H.; Çeliktutan, O.; Gökberk, B.; Sankur, B.; Akarun, L. Bosphorus database for 3D face analysis. In Proceedings of the Biometrics and Identity Management: First European Workshop, BIOID 2008, Roskilde, Denmark, 7–9 May 2008; Revised Selected Papers 1. Springer: Berlin/Heidelberg, Germany; pp. 47–56.
45. Deng, J.; Guo, J.; Ververas, E.; Kotsia, I.; Zafeiriou, S. Retinaface: Single-shot multi-level face localisation in the wild. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, Seattle, WA, USA, 13–19 June 2020; pp. 5203–5212.
46. Deng, J.; Guo, J.; Xue, N.; Zafeiriou, S. Arcface: Additive angular margin loss for deep face recognition. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, Long Beach, CA, USA, 15–20 June 2019; pp. 4690–4699.
47. Lin, D.; Hilbert, N.; Storer, C.; Jiang, W.; Fan, J. Uface: Your universal password that no one can see. *Comput. Secur.* **2018**, *77*, 627–641. [CrossRef]
48. Kähler, O.; Prisacariu, V.A.; Ren, C.Y.; Sun, X.; Torr, P.; Murray, D. Very high frame rate volumetric integration of depth images on mobile devices. *IEEE Trans. Vis. Comput. Graph.* **2015**, *21*, 1241–1250. [CrossRef] [PubMed]
49. Geiger, A.; Ziegler, J.; Stiller, C. Stereoscan: Dense 3d reconstruction in real-time. In Proceedings of the 2011 IEEE Intelligent Vehicles Symposium (IV), Baden-Baden, Germany, 5–9 June 2011; pp. 963–968.
50. Deng, Y. Deep learning on mobile devices: A review. *Mob. Multimed. Image Process. Secur. Appl.* **2019**, *10993*, 52–66.
51. Chen, Y.; Zheng, B.; Zhang, Z.; Wang, Q.; Shen, C.; Zhang, Q. Deep learning on mobile and embedded devices: State-of-the-art, challenges, and future directions. *ACM Comput. Surv. (CSUR)* **2020**, *53*, 1–37. [CrossRef]