UNIVERSITY OF THE AEGEAN

DEPT. OF INFORMATION AND COMMUNICATION SYSTEMS ENGINEERING

Master's Thesis

Identity and Access Management for e-Government Services in the European Union – State of the Art Review

Giannis Konstantinidis

UNIVERSITY OF THE AEGEAN

DEPT. OF INFORMATION AND COMMUNICATION SYSTEMS ENGINEERING

Master's Thesis

Identity and Access Management for e-Government Services in the European Union – State of the Art Review

Διαχείριση Ταυτότητας και Πρόσβασης στις Υπηρεσίες Ηλεκτρονικής Διακυβέρνησης στην Ευρωπαϊκή Ένωση – Ανασκόπηση Τρεχουσών Εξελίξεων

Author: Giannis Konstantinidis
Supervisor: Prof. Dr. Spyros Kokolakis
Submission Date: 25 June 2021

I confirm that this thesis is my own work and I have documented all sources and material used.

Samos, 25 June 2021 Giannis Konstantinidis

Acknowledgements

I feel that the conducting of this thesis has been an unusual experience amidst the coronavirus pandemic. Admittedly, the pandemic has brought multiple challenges and caused unprecedented changes to our everyday lives. Regardless, I believe this experience has motivated me to improvise and focus on living in the moment.

Personal

I would like to thank my family for their continuous support and encouragement during my academic and professional endeavours.

Institutional

I would also like to thank Prof. Dr. Spyros Kokolakis for his consistent advice, guidance, and teachings at the University of the Aegean.

Abstract

Identity and Access Management (IAM) concepts, principles, mechanisms, and technologies help ensure that the right individuals can access the right resources at the right times for the right reasons. They act as the foundation for supporting the objectives of public and private sector organizations regarding information security, privacy, and data protection. Research papers and industrial publications provide much content regarding IAM. However, they typically focus on specific IAM matters and refrain from delivering an overview of the comprehensive domain. There are also a few references to the area of e–government. This thesis intends to consolidate the fundamental aspects of IAM, determine the emerging approaches to IAM, and correlate with the advancement of e–government in the European Union (EU).

IAM programs usually contain components that relate to administration, authentication, authorization, and federation. Moreover, they might intertwine with the Identity Governance and Administration (IGA) and Privileged Access Management (PAM) domains. The emergence of disruptive technologies allows for improvements and new features in IAM, IGA, and PAM. Their state of the art capabilities address the challenges of the expanded threat landscape. They also contribute to safeguarding privacy, increasing efficiency, enhancing user experience, and decreasing administrative tasks. It is challenging to access and analyze the exact IAM specifications of the different EU member states. Nonetheless, the European Commission (EC) acknowledges the developments in the field of digital identity. Its latest policy developments and initiatives set the path towards improving the efficiency of the public sector and strengthening the security posture across the entire EU.

Keywords: Identity and Access Management, e–Government, State of the Art

Περίληψη

Οι έννοιες, οι αρχές, οι μηχανισμοί και οι τεχνολογίες Διαχείρισης Ταυτότητας και Πρόσβασης (Identity and Access Management – IAM) διασφαλίζουν ότι τα σωστά άτομα μπορούν να έχουν πρόσβαση στους σωστούς πόρους τη σωστή στιγμή για τους σωστούς λόγους. Λειτουργούν ως το θεμέλιο για την υποστήριξη των στόχων των οργανισμών του δημόσιου και του ιδιωτικού τομέα σχετικά με την ασφάλεια των πληροφοριών, την ιδιωτικότητα και την προστασία των προσωπικών δεδομένων. Οι επιστημονικές έρευνες και οι βιομηχανικές δημοσιεύσεις παρέχουν αρκετό περιεχόμενο σχετικά με την περιοχή του IAM. Ωστόσο, συνήθως επικεντρώνονται σε συγκεκριμένα ζητήματα και αποφεύγουν να παρέχουν μια ολοκληρωμένη επισκόπηση. Ταυτόχρονα, υπάρχουν ελάχιστες συσχετίσεις με τον τομέα της ηλεκτρονικής διακυβέρνησης. Αυτή η μεταπτυχιακή διπλωματική εργασία σκοπεύει να ενοποιήσει τις θεμελιώδεις πτυχές του IAM, να καθορίσει τις τρέχουσες εξελίξεις στο IAM και να τις συσχετίσει με την ανάπτυξη της ηλεκτρονικής διακυβέρνησης στην Ευρωπαϊκή Ένωση (ΕΕ).

Τα προγράμματα IAM συνήθως περιέχουν στοιχεία που σχετίζονται με τη διαχείριση (administration), την αυθεντικοποίηση (authentication), την εξουσιοδότηση (authorization) και την ομοσπονδία (federation) των ταυτοτήτων. Επιπλέον, τείνουν να συνδέονται με τους τομείς της Διακυβέρνησης και Διαχείρισης Ταυτότητας (Identity Governance and Administration – IGA) και της Διαχείρισης Προνομιακής Πρόσβασης (Privileged Access Management – PAM). Οι σύγχρονες τεχνολογίες επιτρέπουν βελτιώσεις και νέα χαρακτηριστικά στα συστήματα IAM, IGA και PAM. Οι προηγμένες δυνατότητες τους αντιμετωπίζουν τις προκλήσεις του διευρυμένου τοπίου απειλών (threat landscape). Συμβάλλουν επίσης στην προστασία της ιδιωτικότητας, στην αύξηση της αποτελεσματικότητας, στην ενίσχυση της εμπειρίας των χρηστών και στη μείωση των χειροκίνητων εργασιών. Η πρόσβαση στις ακριβείς προδιαγραφές IAM των διαφόρων κρατών μελών της ΕΕ, καθώς και και η αναλύση τους, είναι δύσκολη. Σε κάθε περίπτωση, η Ευρωπαϊκή Επιτροπή αναγνωρίζει τις εξελίξεις στον τομέα της ψηφιακής ταυτότητας. Οι τελευταίες εξελίξεις στην χάραξη των πολιτικών και οι πρωτοβουλίες της Επιτροπής αποσκοπούν στη βελτίωση της αποτελεσματικότητας του δημόσιου τομέα και στην ενίσχυση του επιπέδου ασφαλείας σε ολόκληρη την ΕΕ.

Λέξεις–Κλειδιά: Διαχείριση Ταυτότητας και Πρόσβασης, Ηλεκτρονική Διακυβέρνηση, Τρέχουσες Εξελίξεις

Contents

List of Figures

List of Tables

List of Acronyms

ABAC . . . . . Attribute–Based Access Control

ABE . . . . . Attribute–Based Encryption

ACL . . . . . Access Control List

AES . . . . . Advanced Encryption Standard

AI . . . . . Artificial Intelligence

AIA . . . . . Artificial Intelligence Act

AM . . . . . Access Management

API . . . . . Application Programming Interface

CSIRT . . . . . Computer Security Incident Response Team

DAC . . . . . Discretionary Access Control

DL . . . . . Deep Learning

EBP . . . . . European Blockchain Partnership

EBSI . . . . . European Blockchain Services Infrastructure

EC . . . . . European Commission

eIDAS . . . . . Electronic Identification, Authentication and Trust Services

ENISA . . . . . European Network and Information Security Agency

ESSIF . . . . . European Self–Sovereign Identity Framework

EU . . . . . European Union

FIM . . . . . Federated Identity Management

IAM . . . . . Identity and Access Management

IBE . . . . . Identity–Based Encryption

IdM . . . . . Identity Management

IdP . . . . . Identity Provider

IGA . . . . . Identity Governance and Administration

IIA . . . . . Inception Impact Assessment

ILM . . . . . Identity Lifecycle Management

IMG . . . . . Identity Management and Governance

ITU . . . . . International Telecommunication Union

JIT . . . . . Just–In–Time

JML . . . . . Joiners, Movers and Leavers

JWT . . . . . JSON Web Token

LDAP . . . . . Lightweight Directory Access Protocol

MAC . . . . . Mandatory Access Control

MFA . . . . . Multi–Factor Authentication

ML . . . . . Machine Learning

NIS . . . . . Network and Information Security

NIST . . . . . National Institute of Standards and Technology

OIDC . . . . . OpenID Connect

PAM . . . . . Privileged Access Management

PoLP . . . . . Principle of Least Privilege

RBAC . . . . . Role–Based Access Control

RP . . . . . Relying Party

SAML . . . . . Security Assertion Markup Language

SFA . . . . . Single–Factor Authentication

SLO . . . . . Single Log–Out

SoD . . . . . Separation of Duties

SP . . . . . Service Provider

SSI . . . . . Self–Sovereign Identity

SSO . . . . . Single Sign–On

ZSP . . . . . Zero Standing Privileges

ZTA . . . . . Zero Trust Architecture

ZTM . . . . . Zero Trust Model

1 Introduction

1.1 Background

The remarkable evolution of technology during the past decades has impacted the growth of digital identity. People use their digital identities whenever communicating with one another, accessing online platforms, and engaging in transactions. The influence of digital identities spans across the technological, social, and economic dimensions [1]. Hence, nowadays, multiple Internet–based services such as instant messaging, social networking, and e–banking revolve around digital identities.

Digital identities are an indispensable component of modern e–government applications. Like analogue identities (e.g., national identity documents), public and private sector organizations recognize digital identities and determine whether the persons they are transacting with are indeed the ones they claim to be [2]. Alongside their significant involvement in the authentication and authorization processes, digital identities function as virtual containers and incorporate the diverse attributes (e.g., names, addresses, and national identification numbers) that characterize people.

Identity and Access Management (IAM) is the collective term for policies and technologies that enable the right individuals to access the right resources at the right times for the right reasons [3]. As the name suggests, IAM is responsible for the comprehensive management of digital identities and the appropriate enforcement of Access Management (AM). The broader discipline emerged alongside Internet–based and network–based services around the beginning of the 21st century. The establishment of IAM facilitates the participation of digital identities in an extensive range of transactions and contributes to the multiple interests of the respective stakeholders [4]. However, IAM is often difficult to understand due to its extensive range of functionalities and configurations. Thus, IAM requires considerable effort in planning, deploying, and adjusting.

1.2 Problem Statement

In general, public sector organizations rely on large–scale information and communication systems for their operations. They tend to manage heterogeneous computing environments where dissimilar hardware and software products co–exist. In parallel to the

challenges on information security that might arise from legacy and non–interoperable technological solutions, end–users and system administrators feel overwhelmed whenever accessing disconnected systems and performing repetitive tasks [5]. Accordingly, IAM can act as the foundation for streamlining the management of identity information across different systems, unifying the authentication and authorization procedures of different categories of end–users, ensuring the consistent application of security policies, and enhancing the broader end–user experience.

The technological evolution, including the reliance of e–government services on cloud computing, brings unique challenges and necessitates adjustments to IAM [6]. As a response, for instance, the evolvement of perimeterless approaches to information security enhances the administration of digital identities and the management of contextual access. Reasonably, professionals in industry and academia progress with their research and development efforts. Their contributions lead to improvements in IAM. Although IAM is considered an indispensable component of modern e–government services, the leading academic search engines and databases include a few up–to–date sources that connect the two domains. Moreover, there are limited references to the current IAM specifications of e–government services across the EU. Consequently, it appears there is insufficient information on the relevance of the state of the art IAM capabilities with the e–government domain.

Recently, the emergence of COVID–19 as a global pandemic has disrupted multiple industries, deranged supply chains, and imposed teleworking. The phenomenon brings significant risks concerning information security, business continuity, and resilience [7]. Unquestionably, governments prioritize the well–being of their citizens and implement measures to help reduce the spread of the virus. Meanwhile, the accelerating pace of digital transformation and the increasing use of collaborative software impose challenges on information security, privacy, and data protection. Hence, the pandemic has stressed the importance of IAM in safeguarding remote access and improving the security posture of public and private sector organizations [8]. The investments in emerging technologies support the planning and rollout of adaptive IAM strategies. Nevertheless, the responses of e–government services in the EU remain somewhat unclear.

1.3 Scope and Objectives

The purpose of this master's thesis is to explore the fundamental IAM aspects for e–government services, identify the emerging approaches to IAM, and examine the direction of the EU towards the state of the art IAM concepts, principles, mechanisms, and technologies. Thus, the main objectives of this thesis correspond as follows:

- Study and organize the available literature (e.g., academic papers, technical stan–

dards, and industrial publications), with an emphasis on relevant content that has been written during the last ten years;
- Provide an up–to–date overview of the established approaches to IAM that meanwhile associate with e–government services;
- Expand upon the overview of the IAM landscape and indicate the emerging approaches to IAM that contribute to e–government services; and
- Examine the most recent policy developments and corresponding initiatives at an EU level and correlate them with the emerging approaches to IAM.

1.4 Assumptions and Limitations

This master's thesis draws bibliographic references from academic search engines and databases such as Google Scholar, Scopus, and HEAL–Link that consolidate a plethora of academic content (e.g., conference papers, journal entries, and book chapters). Nevertheless, the author acknowledges that the before–mentioned platforms might prevent access to specific material due to the applicability of restriction policies or licensing constraints. This situation impacts the preparation of this thesis.

IAM is an extensive domain that consists of multiple concepts, principles, mechanisms, and technologies. This master's thesis intends to highlight the conventional and innovative approaches to establishing IAM features. There are already individual references to the technical specifications and procedures of particular IAM components. Therefore, the thesis consolidates such separate references and provides an overview of the comprehensive IAM landscape. Nonetheless, due to time constraints, the author does not opt for presenting an exhaustive list of IAM–related aspects.

With regard to the relationship between IAM and e–government, it appears that the majority of the relevant research items are out–of–date. In essence, the case study reviews of the previous decade—which discuss the capacities of e–government services for IdM and IAM—no longer reflect the current state. Hence, the author believes it is unnecessary to examine such content. On the one hand, there is the possibility of conducting up–to–date case studies. On the other hand, this opportunity presupposes the obtainment of documentation and the scheduling of interviews with system engineers and architects to obtain an increased understanding of the exact IAM capabilities. As there might be confidentiality requirements in place and due to time restrictions, the author decides to examine the relevant policy developments and initiatives of the EU.

Currently, there are different opinions on the relationships among IAM, Identity Governance and Administration (IGA) or Identity Management and Governance (IMG), and Privileged Access Management (PAM). The author assumes that these domains indeed associate with one another, although he does not investigate the matter further. This

master's thesis focuses primarily on IAM but also references IGA and PAM capabilities.

1.5 Thesis Structure

The current chapter serves as an introduction to this master's thesis. It establishes the essential background information for understanding the extensive IAM domain. Moreover, the chapter outlines the problem statement, explains the scope and objectives, and reveals the assumptions and limitations regarding the thesis.

The following chapter makes an introduction to the fundamental aspects of IAM for e–government services. It considers a diverse set of concepts, principles, mechanisms, and technologies that fall under identity administration, authentication, authorization, and federation. Also, the chapter references some characteristics of IGA and PAM.

The third chapter concentrates on the emerging approaches to IAM for e–government services. It highlights the state of the art concepts, principles, mechanisms, and technologies that support identity administration, authentication, and authorization. Furthermore, the third chapter features several aspects related to IGA and PAM and discusses the direction towards the future of IAM.

The fourth chapter reflects some of the latest EU policies and initiatives and associates them with the emerging approaches to IAM. It intends to present a high–level overview of how the EU member states respond to the need for advanced IAM features.

The fifth chapter reflects the contributions of this master's thesis and concludes with potential recommendations for future research.

2 Fundamental Aspects

2.1 Digital Identity

According to the bibliographic sources, there are different definitions of digital identity. In the context of IAM, it is acceptable that identities represent the distinct characteristics of entities. In particular, the International Telecommunication Union (ITU) establishes that an identity contains one or more attributes that can sufficiently distinguish an entity or entities within context [9]. Similarly, the National Institute of Standards and Technology (NIST) supports that an identity is an attribute or a set of attributes that can uniquely describe a subject within a given context [10]. Moreover, the International Organization for Standardization (ISO) expands upon the before–mentioned definitions and assumes that an entity can relate to multiple identities and that several entities can share the same identity [11]. Understandably, an entity does not always mean some natural person—the existence of non–human identities (e.g., bots) is permissible. Nonetheless, this thesis means to focus on the representation of human identities.

Identities consolidate different kinds of attributes. They frequently include attributes that are universal across entities (e.g., name and address). Depending on the circumstances, it might be challenging to identify an entity based solely on non–unique attributes. Therefore, unique identifiers (e.g., passport number or employee number) play an important role in distinguishing one entity from another.

Figure 2.1 illustrates the relationships among entities, identities, identifiers, credentials, and attributes. An entity can relate to more than one identity. Each identity incorporates attributes that describe the respective entity. Besides, each identity contains at least one unique identifier for distinguishing itself and involves credentials for authentication purposes.

2.2 Identity and Access Management

Identity Management (IdM) associates with IAM to the extent that people use these terms interchangeably [13]. However, there are subtle differences between them. IAM is essentially the superset that includes both IdM and AM elements. Accordingly, organizations deploy all–around IAM systems to streamline the administration of identities

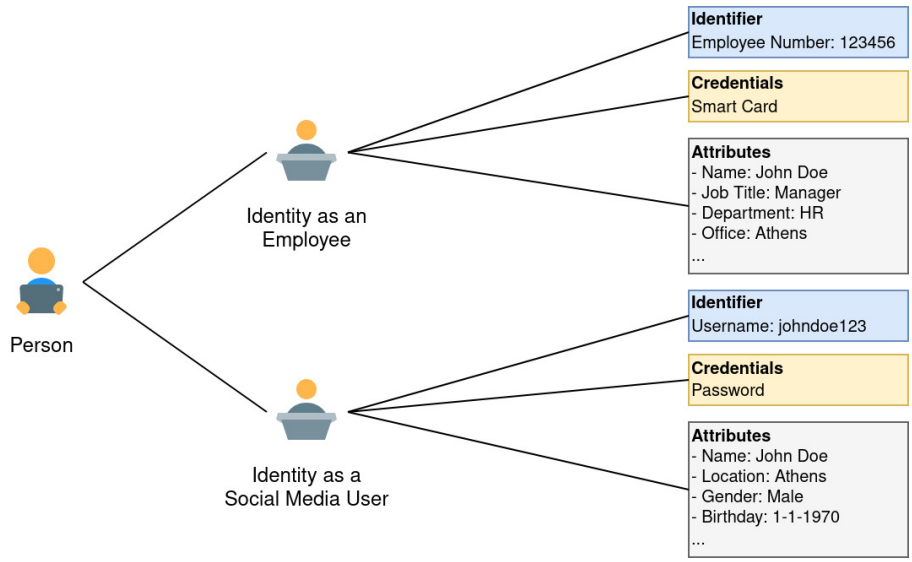

Figure 2.1: Identities, Identifiers, Credentials and Attributes — Adapted [12]

and improve the control of access to their resources.

IAM intertwines with IGA and PAM. IGA systems further the standard identity administration capabilities of IAM systems and enable organizations to obtain increased visibility over identities. They also support administrators in streamlining ILM, reviewing and adjusting access, automating workflows, and assessing compliance [14]. Meanwhile, PAM systems complement IAM systems regarding human and non–human identities with privileged (i.e., elevated) access to resources. As unmanaged privileged accounts might lead to significant attack vectors, PAM systems assist in regulating privileged access, flagging high–risk activity, monitoring sessions, and managing approvals [15]. The first chapter clarifies that the entire thesis focuses on IAM. At the same time, however, it references some aspects of IGA and PAM.

Before exploring the IAM domain, it is meaningful to discuss the roles of the Identity Provider (IdP) and the Service Provider (SP). Usually, the IdP is either a discrete system or a service orchestrated by an all–around IAM system that facilitates the creation, maintenance, and management of digital identities. The IdP generates and assigns identity attributes, performs the correlation between identity attributes, offers assertions about identity attributes, and provides the necessary credentials for identity attributes and identity assertions [16]. Consequently, the SP (e.g., web application or native application) needs to receive some positive assertion from the IdP before admitting an entity [17]. Alternatively, people often refer to the SP as the Relying Party (RP).

The literature suggests that three approaches for IAM have evolved over the years,

with each of them corresponding to different use–cases [18]:

- Centralized (network–centric), which considers one environment (i.e., one IdP and potentially multiple SPs within the same environment);
- Federated (application–centric), where different environments establish trust relationships for the secure exchange of identity information; and
- Decentralized (user–centric), which leverages disruptive technologies (e.g., distributed ledgers) to provide entities with additional control over their identities.

The current chapter discusses the centralized and federated approaches to IAM. The following sections and subsections explore the traditional practices of identity administration, authentication, authorization, and federation. As far as the decentralized approach is concerned, the next chapter provides baseline information about the relationship between blockchain and IAM.

2.2.1 Administration

The evolvement of IAM reflects modern technologies that contribute to the administration of identities. Reasonably, the emergence of IGA combines identity governance with identity administration capabilities and contributes to expanding the traditional boundaries of IAM. There are specific differences between IAM and IGA, although the two domains align their responsibilities concerning identity administration.

Figure 2.2 provides an example scenario of identity administration in the context of e–government. This high–level diagram assumes that the user (e.g., citizen or public sector employee) goes through the registration department before accessing any e–government services. The IAM system regularly fetches information about identities from the respective authoritative source. It proceeds with provisioning, thereby facilitating the creation and update of accounts in the appropriate SPs. Furthermore, the IAM system is responsible for reconciling identity information, meaning that it scans for inconsistencies between identities and the corresponding accounts. If required, the IAM system also triggers the de–provisioning process and ensures the necessary account removals at the level of the SPs.

2.2.1.1 Authoritative Sources

The establishment of all–around IAM systems requires their connection to the authoritative sources that act as the source of truth for identities. An authoritative source serves as the repository for the representation, storage, and administration of identity information and may additionally incorporate mechanisms for accessing such information [19]. Directory services such as Microsoft Active Directory and OpenLDAP are examples of

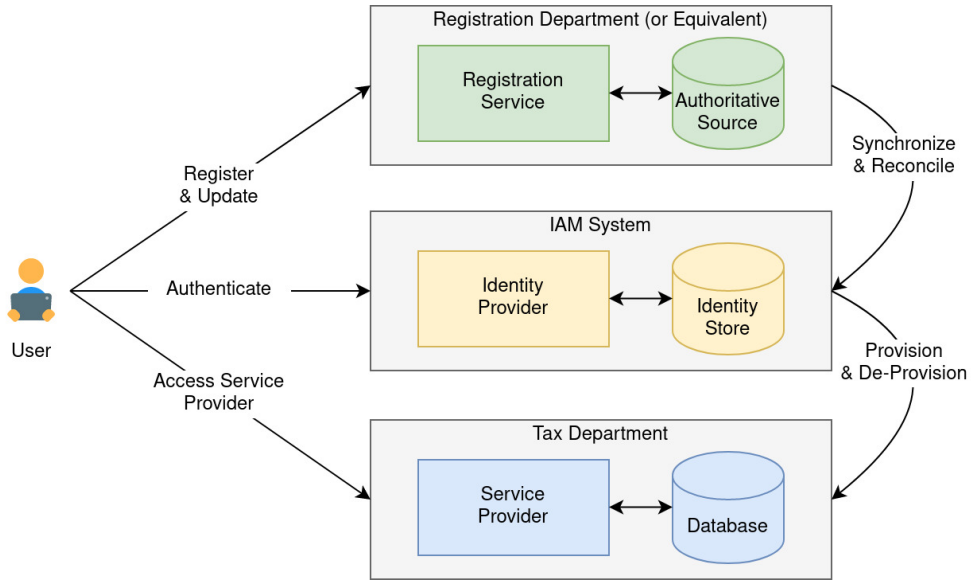

Figure 2.2: Identity Administration Architecture

authoritative sources that embrace the Lightweight Directory Access Protocol (LDAP). In practice, IAM systems usually feature software connectors and provide substantial documentation for performing the necessary integrations. Though, there are organizations that might keep specific resources disconnected from their networks for various reasons. In that case, IAM systems might additionally support importing identity information from flat files (e.g., CSV and XML).

2.2.1.2 Identity Lifecycle

As IAM systems are in charge of managing digital identities throughout different stages, they constantly engage with the concept of Identity Lifecycle Management (ILM). In essence, every IAM system is responsible for [20]:

- Creating identities, by collecting and registering the relevant attributes, defining the necessary credentials, and issuing the identities;
- Facilitating the use of identities in electronic transactions, provided that the required security controls are in place;
- Updating identities whenever there are attributes that require corrections or modifications; and
- Revoking identities, which corresponds to either suspending particular identity attributes or permanently removing identities.

IAM systems have diverse specifications and technical components. Thus, there are various approaches to the analysis, design, and implementation of ILM. Regardless, IAM practitioners analyze multiple scenarios for Joiners, Movers and Leavers (JML) as a prerequisite. JML refers to the entities that enter an organization, transfer within an organization or across organizations, or leave an organization respectively.

2.2.1.3 Provisioning and De–Provisioning

The provisioning mechanism relates to authoritative sources, ILM, and JML. Provisioning is triggered, for instance, as soon as the IAM system detects changes (e.g., joiner's information added or mover's information modified) in the corresponding authoritative source. Whenever provisioning occurs, the IAM system employs the necessary means of connectivity and contributes to the delivery of the right level of access to the right resources [21]. The IAM system provisions identities and triggers the formulation of accounts in the specified SPs. It also arranges the modification of existing accounts, provided that the relevant changes are detected beforehand.

De–provisioning is another mechanism that is somewhat the opposite of provisioning. If an entity leaves the organization either manually or automatically (e.g., the contract of an employee ends without being extended), the IAM system facilitates the suspension or the removal of any accounts associated with that identity.

Provisioning and de–provisioning are significant components of the different workflows that are configurable within IAM systems. Such workflows contribute to the consistent and streamlined execution of the ILM tasks and, if required, may trigger approval processes (e.g., require manager approval) to enforce control [22].

Figure 2.3 illustrates an example scenario that may emerge as an appropriate workflow. It defines the onboarding of new joiners. As soon as the user (e.g., citizen or public sector employee) finishes their registration, the IAM system fetches the information and checks for any omissions and inconsistencies. If there are no restrictions, the IAM system creates the identity and initiates the provisioning process. Then, the relevant SPs create the accounts with the necessary permissions. Finally, the IAM system might notify the user regarding their successful onboarding and provide further instructions (e.g., documentation and support contacts).

2.2.2 Authentication

Authentication is the process that determines whether an identity belongs to an entity. IAM systems may feature an authentication service (e.g., alongside the responsibilities of the IdP) or may alternatively delegate the authentication process to another system instead—for the second scenario, the trusted relationship between the two systems is a

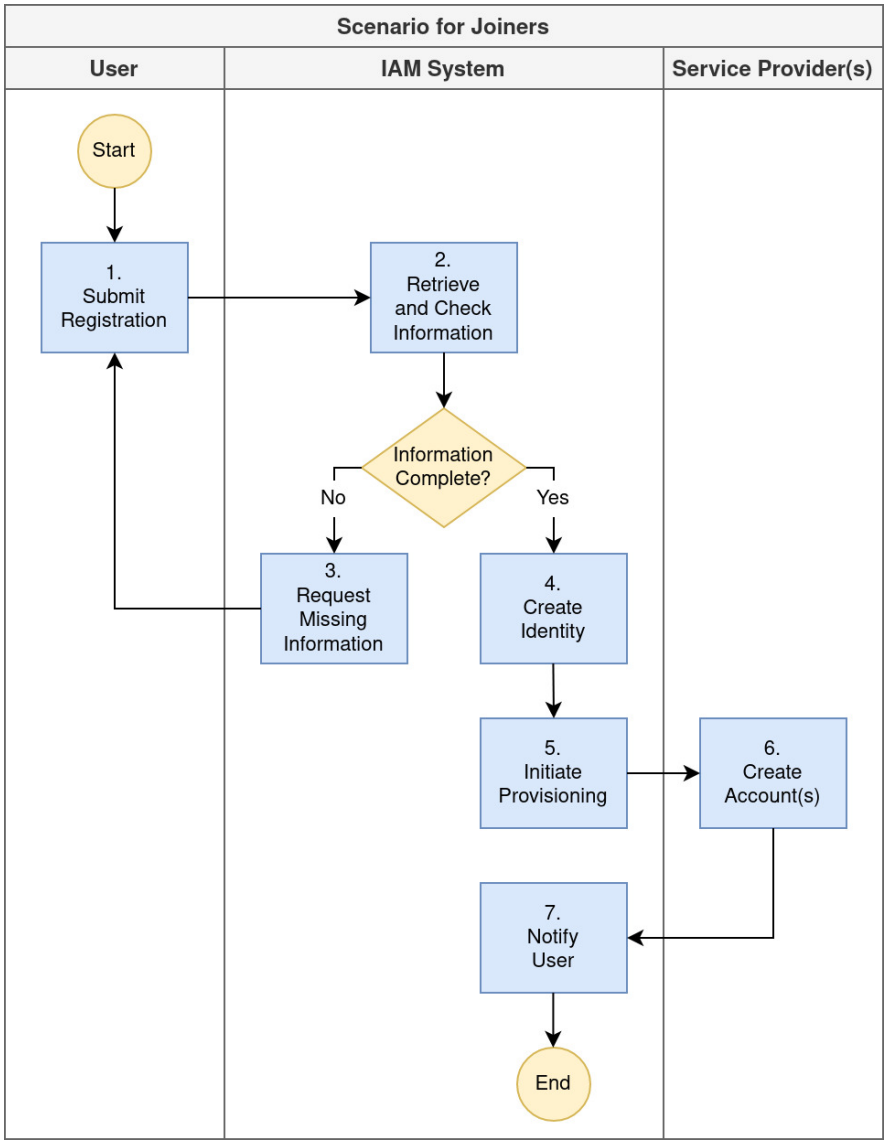

Figure 2.3: Scenario for Joiners

prerequisite. Before entities can transact with the SP of their choice, they normally have to go through the authentication process during which they provide credentials in order to prove their identity. There are currently three high–level categories of credentials which are better known as factors of authentication [23]:

- Something–you–know, according to which the entity needs to supply something stored in their memory (e.g., password or PIN code);
- Something–you–have, which expects the entity to use some physical item (e.g., security token or smartcard) in their possession; and
- Something–you–are, which analyzes the human characteristics (i.e., physical or behavioural biometrics) of the entity.

2.2.2.1 Single–Factor Authentication

Single–Factor Authentication (SFA) relies upon one factor of authentication. This term is sometimes used interchangeably with password–based authentication, although SFA does not always correspond to passwords or security questions. Instead, authentication processes can depend on security devices (e.g., swipe cards and smart cards) or employ biometrics (e.g., voice recognition and facial recognition) as appropriate.

Information security professionals may assume that one factor of authentication is analogous to one line of defence around authentication. In the case of password–based authentication, the combination of weak passwords and poor password management practices is exceptionally problematic as entities often use the same passwords that malicious entities can predict or steal [24]. As far as security devices are concerned, they are equally prone to be lost or stolen and therefore depending entirely on them for authentication purposes raises uncertainties. Alternatively, biometrics provide convenience to end–users but are more troublesome to maintain, raise privacy concerns, and are equally subject to attacks (e.g., spoofing) [25].

2.2.2.2 Multi–Factor Authentication

Multi–Factor Authentication (MFA) extends the requirements of SFA and introduces more than one authentication technique [26]. The primary purpose behind the configuration of MFA is to establish some layered defence and reduce the likelihood of fraudulent activity such as identity theft.

Two–Factor Authentication (2FA) is the term that implies two authentication techniques and often appears alongside MFA. The main difference between SFA and MFA is that the latter indicates multiple (i.e., more than one) authentication factors in general. As a consequence, 2FA can be regarded as MFA but not always the opposite. There

is no common ground on whether the enforcement of 2FA or MFA needs to involve distinct factors (e.g., something–you–know and something–you–have instead of two counts of something–you–know), although NIST endorses this approach for particular use–cases such as e–commerce transactions [27].

2.2.2.3 Step–Up Authentication

Step–up authentication is the process that triggers authentication challenges under specific conditions [28]. For instance, if an entity attempts to access high–risk resources (e.g., transfer money through an e–banking service), step–up authentication requires them to respond to an SFA or MFA challenge and prove their identity again. Normally, as long as an authenticated entity accesses low–risk resources, they are not subject to step–up authentication.

2.2.2.4 Adaptive Authentication

Adaptive authentication, also known as risk–based authentication, is comparable to step–up authentication as it also presents entities with SFA or MFA challenges. The main difference is that adaptive authentication considers contextual and dynamic factors such as IP addresses, date and time, physical locations, and device information [29]. For example, whenever an entity attempts to perform any activity while connected from an unusual IP address, the adaptive authentication process takes the preconfigured authentication factors into account and triggers an authentication challenge.

2.2.3 Authorization

Authorization is the process of determining whether an entity can perform a particular action (e.g., accessing resources) upon successful authentication. There are several elements that pertain to authorization. This subsection examines two authorization principles as well as the purposes of access control models.

2.2.3.1 Principle of Least Privilege

The Principle of Least Privilege (PoLP) dictates that entities receive the minimum amount of permissions needed to perform their duties. Modern–day cyberattacks often exploit excess privileges (e.g., some database administrator has access to domain controllers), so the proper enforcement of PoLP helps reduce the broader attack surface.

The idea behind PoLP sounds simple, though there are usually technical considerations that make its implementation complicated. The challenges around PoLP may occur because, nowadays, both public and private sector organizations tend to [30]:

- Operate several computing environments (e.g., on–premises, cloud, and hybrid);
- Practice different operating systems (e.g., Microsoft Windows and GNU/Linux);
- Include numerous endpoints (e.g., desktops, laptops, and smartphones); and
- Manage different kinds of identities (e.g., human and non–human identities).

2.2.3.2 Separation of Duties

The Separation of Duties (SoD), also known as the Segregation of Duties, is an authorization principle that requires more than one person for performing high–risk activities. SoD seeks to prevent entities from obtaining excessive control over the processes and assets of their organization. Such entities may be single individuals or even groups of individuals. Based on their particular needs, organizations can implement SoD as [31]:

- Individual–Level SoD, which is the most popular type of SoD and expects the collaboration between separate individuals whenever there are conflicting tasks (e.g., the administrator requires approval from the line manager before onboarding new joiners);
- Unit–Level SoD, where different functions of the organization work together to perform incompatible duties (e.g., the HR department submits payroll data and the finance department proceeds with payments); and
- Organization–Level SoD, where different organizational entities participate in performing conflicting operations (e.g., an external audit performed by an independent firm).

2.2.3.3 Access Control Models

Information security professionals might suggest that access control is the superset that contains both authentication and authorization elements. Regardless, this subsection discusses access control models in particular rather than the extensive category of access control. Towards the purposes of this master's thesis and for the sake of simplicity, the author assumes that access control models come under authorization. In practice, organizations configure such mechanisms for controlling access to their resources.

Mandatory Access Control (MAC) and Discretionary Access Control (DAC) are two well–established models that are enforceable within systems. MAC allows or denies access to resources based on predefined sets of rules (i.e., clearance levels), whereas

DAC enables each resource owner to specify who receives access [32]. Nevertheless, organizations can use MAC in conjunction with DAC to balance control and flexibility.

Role–Based Access Control (RBAC) is another model that shares a few similarities with MAC as they both practice non–discretionary access control. In contrast to the clearance levels of MAC, RBAC considers roles that are practically more diverse. The public and private sector organizations that implement RBAC can benefit from decreasing the administrative burden, centralizing the management of roles, increasing the visibility over the access permissions, and reducing the maintenance costs [33]. Eventually, the choice for RBAC leads to maximizing operational efficiency.

2.2.4 Federation

Federated Identity Management (FIM) establishes the cooperation among IdPs and SPs regarding identity processes, policies, and technologies [34]. Admittedly, there is no universal approach to identity federation because the exact technical specifications differ across organizations. Notwithstanding, the essential requirement for FIM is the establishment of trust relationships before the IdPs can communicate with the relevant SPs to exchange identity information as necessary. Towards FIM, the popular authentication and authorization standards such as the Security Assertion Markup Language (SAML), OAuth, and OpenID Connect (OIDC) play an indispensable role.

SAML is an open standard for the exchange of authentication and authorization information between IdPs and SPs. It transfers assertions that serve as authentication, attribute, and authorization decision statements [35]. Admittedly, SAML might require significant effort to implement. In opposition to SAML, OAuth is primarily an authorization framework for providing access to protected resources across services. It facilitates the delegation of authorization, strengthens the security of Application Programming Interface (API) requests, and enables administrators to track the use of access tokens [36]. Meanwhile, OIDC emerges as an authentication layer on top of the OAuth protocol that enables SPs to delegate the authentication of entities to OAuth authorization servers. Modern applications that emphasize APIs can capitalize on the benefits of using OAuth in conjunction with OIDC [37]. Nevertheless, the choice between SAML and OAuth with OIDC depends on the exact technical requirements of organizations.

Figure 2.4 depicts an example of identity federation in the area of e–government. The IdP stores the identity information in the respective identity store. The user accesses the SPs that rely upon the IdP to send the necessary assertions upon successful authentication. SPs preserve databases for data storage, although FIM helps eradicate the fragmentation of identities. In the meantime, it enhances the end–user experience.

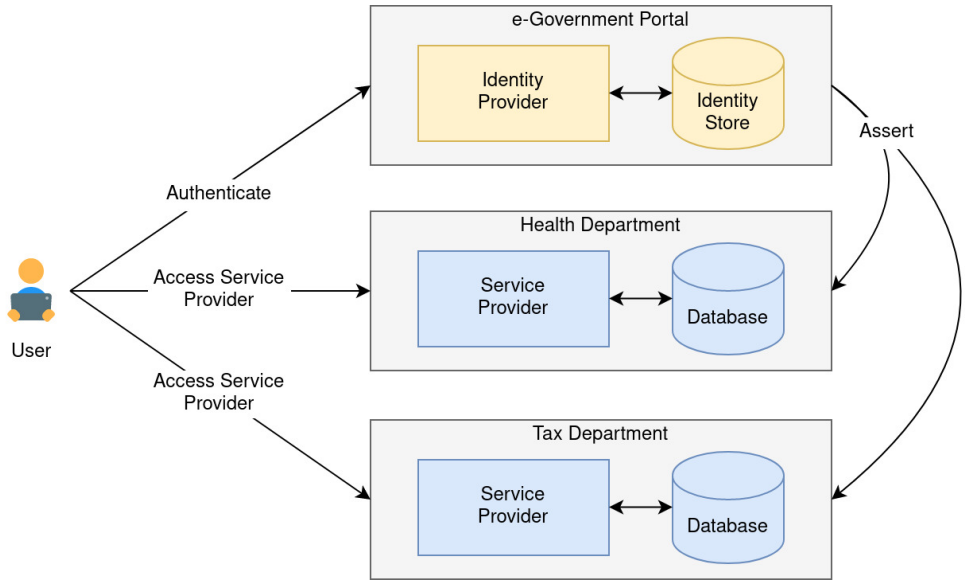

Figure 2.4: Identity Federation Architecture — Adapted [38]

2.2.4.1 Single Sign–On

Single Sign–On (SSO) is an authentication method that allows entities to access multiple SPs simultaneously by using the same set of credentials. Likewise, Single Log–Out (SLO) terminates the access to all SPs at once. SSO falls under FIM but concentrates on one organizational domain [39]. SSO relates to FIM, whereas FIM does not necessarily correspond to SSO.

2.3 Chapter Summary

The second chapter of this master's thesis explores the fundamental aspects of IAM, clears up some common misconceptions, and builds the necessary background knowledge before proceeding with the state of the art review. Table 2.1 outlines some of the terms that the second chapter references.

The definitions of digital identity tend to differ slightly. Nonetheless, identities represent the different characteristics of entities. They carry identifiers for distinguishing entities, credentials for authenticating entities, and attributes for describing entities.

IAM is the superset that includes IdM and AM. IAM connects with IGA and PAM. IdPs create, maintain, and manage digital identities, whereas SPs rely upon the information from IdPs to admit entities and regulate their activities. There are three potential approaches to IAM—namely, the centralized (network–centric), the federated

(application–centric), and the decentralized (user–centric) approach.

The intention of identity administration is to streamline the management of identity information across the organization. The authoritative sources act as the source of truth for identities and provide up–to–date information. IAM systems are responsible for creating identities, facilitating the use of identities in electronic transactions, updating identities, and revoking identities. There are different approaches to performing ILM, although they typically revolve around JML scenarios. The provisioning and de–provisioning mechanisms assist in creating, updating, suspending, or removing accounts depending on the exact circumstances.

Authentication determines whether an identity belongs to an entity. The three main factors of authentication are something–you–know, something–you–have, as well as something–you–are. SFA depends on one factor of authentication, while MFA involves additional factors. Step–up authentication is the process that considers static risk factors and triggers authentication challenges as necessary. In contrast, adaptive authentication analyzes contextual and dynamic risk factors.

Authorization decides on the actions an identity can perform. PoLP is the principle that expects the assignment of the minimum amount of permissions. In parallel, the SoD principle requires the involvement of additional entities in high–risk activities. Moreover, the enforcement of access control models such as MAC, DAC, and RBAC takes specific parameters into account and helps in regulating access to resources.

FIM establishes trust relationships among IdPs and SPs for the exchange of identity information. Popular standards such as SAML, OAuth, and OIDC assist with authentication and authorization. SSO belongs to the FIM superset, although FIM does not always correspond to SSO.

Table 2.1: Established Approaches — Summary

Category	Name	Description
Administration	Authoritative Source	The source of truth for identities. It helps represent, store, manage, and access identity information [19].
	Identity Lifecycle Management	The management of identities throughout different stages. In essence, the responsibility of creating, facilitating, updating, and revoking identities [20].

	Provisioning and De–Provisioning	The mechanisms for ensuring the delivery of the right access to the right resources [21]. They aid in creating, updating, suspending, or removing accounts associated with identities.
Authentication	Single–Factor Authentication	The method that relies upon one factor of authentication. It often corresponds to password–based authentication [24], although the use of security devices or biometrics [26] is equally possible.
	Multi–Factor Authentication	The extension of SFA that introduces more than one authentication technique. Ideally, may rely upon different factors of authentication [27].
	Step–Up Authentication	The process that checks the applicability of preconfigured scenarios and triggers authentication challenges [28].
	Adaptive Authentication	The process that triggers authentication challenges while considering contextual and dynamic factors [29].
Authorization	Principle of Least Privilege	The principle that expects the assignment of the minimum amount of permissions. There are technical and operational challenges to its enforcement [30].
	Separation of Duties	The principle that requires more than one person for performing high–risk activities. It supports different approaches [31].
	Access Control Models	The methods of allowing or denying access to resources based on predefined criteria. Popular examples include MAC, DAC, and RBAC [32].
Federation	Federated Identity Management	The practice of establishing the cooperation among IdPs and SPs in identity processes, policies, and technologies [34].
	Single Sign–On	The method for accessing multiple SPs simultaneously with the same set of credentials. SSO implies FIM but not necessarily vice–versa [39].

3 State of the Art Review

3.1 Methodology

This chapter emphasizes some of the latest advancements in IAM that are applicable to e–government services in the EU. Undoubtedly, this master's thesis does not intend to present an exhaustive list of relevant concepts, principles, mechanisms, and tech–nologies. The intention is to point the readers in the direction that the IAM domain is heading. Accordingly, the author defines and adopts an essential methodology for preparing and writing the state of the art review.

Figure 3.1 depicts the methodology for the state of the art review that comprises four sequential steps. First, the thesis helps determine the emerging approaches to IAM by acknowledging the insights provided by research and advisory firms and IAM, IGA, and PAM vendors. Second, the literature search involves browsing through the available content in academic databases and search engines and considering suitable material from IAM, IGA, and PAM vendors. Third, the selection of relevant literature applies two principal criteria: a) each publication dates from 2016 onwards, and b) each topic directly matches at least one of the predetermined emerging approaches to IAM. Four, the actual writing of the state of the review reflects upon the advantages and disadvantages of each approach and meanwhile presents potential research directions.

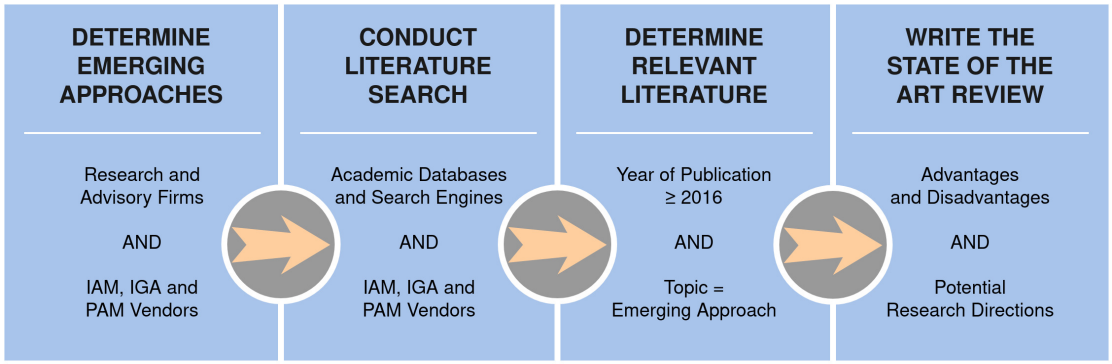

Figure 3.1: State of the Art Review Methodology

3.2 Emerging Approaches

The first subsection covers identity and blockchain that associates with identity administration and IdM. The following subsections introduce the innovative continuous authentication and passwordless authentication processes that—as their names suggest—pertain to authentication. Furthermore, the subsequent subsections reference Attribute–Based Access Control (ABAC), Just–In–Time (JIT) Access, and the Zero–Trust Model (ZTM) that somewhat relate to authorization. Finally, the remaining subsections discuss identity analytics and identity and Artificial Intelligence (AI), respectively, that contribute to identity governance.

3.2.1 Identity and Blockchain

Blockchain technology allows for tamper–resistant data storage while embracing transparency and decentralization. The previous chapter of this thesis discusses the two traditional approaches to IdM, namely the centralized (network–centric) and the federated (application–centric) approaches. Contrarily, blockchain has reinforced the decentralized (user–centric) approach to IdM and shows potential in providing people with improved control over their identity information. Its transparency, auditability, and immutability features can additionally support organizations with fulfilling their data protection obligations and demonstrating compliance [40].

However, blockchain for digital identity has also exposed potential implications to the requirements of regulatory frameworks such as the EU's General Data Protection Regulation (GDPR). Blockchain encourages transparent communications to data subjects (Art. 12 GDPR) and supports the security of data processing (Art. 32 GDPR), although at the same time brings challenges associated with the definition of the purposes and means behind processing (Art. 4 GDPR), the revocation of consent (Art. 7 GDPR), the right to rectification (Art. 16 GDPR), the right of erasure (Art. 17 GDPR), the right to data portability (Art. 20 GDPR), and data protection by design and by default (Art. 25 GDPR) [41]. As a consequence, these contradictions have set the path for further research on GDPR–compliant distributed ledger technologies for IdM [42].

Research has highlighted the importance of the Self–Sovereign Identity (SSI) model (i.e., entities control their identities across boundaries and systems consist of transparent algorithms for the administration of identities) that is rendered possible with blockchain for identity management [43]. Furthermore, the academic community has demonstrated increased interest in novel authentication mechanisms (e.g., using smart contracts as an enabling technology), privacy–preserving schemes for achieving selective anonymity (e.g., zero–knowledge proof approaches), and trust–based digital identity management schemes (i.e., based on the SSI principle) [44]. Aside from digital

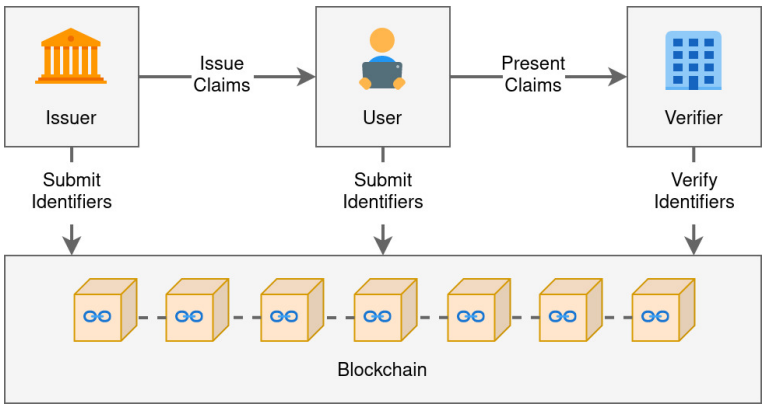

Figure 3.2: Self–Sovereign Identity Architecture — Adapted [46]

identities associated with human users, research has paved the way for blockchain–based IAM for the Internet of Things which provides compatibility with all kinds of de–vices and features tamper–resistant access control [45].

Figure 3.2 illustrates a high–level example of SSI in which the trusted authority first issues credentials and signs them using their decentralized identifier. Then, the user counter–signs those credentials using their decentralized identifier and proceeds with storing them on their device whilst applying strong encryption. Meanwhile, both the is–suer and the user submit the public–key signatures of their identifiers to the blockchain. Consequently, the SP, also known as the verifying authority, receives claims from the user and checks the corresponding blockchain records.

The integration of blockchain with IAM looks promising not only for identity owners but also for the organizations responsible for handling identities. On the one hand, blockchain acts as a catalyst for decentralizing digital identities and circumvents some potential vulnerabilities of traditional IAM systems. On the other hand, blockchain of–fers immutable data storage and thus should not contain personal data. This antithesis indicates that distributed ledgers are most suitable for identity verification purposes us–ing modern cryptography. Individuals are responsible for controlling their data and, consequently, help eradicate massive data breaches that are primarily associated with the centralized and federated approaches to IdM.

3.2.2 Continuous Authentication

The long–established one–shot or one–time authentication processes are responsible for verifying identities once. In practice, they examine the credentials during the initial log–in phase and then decide whether to admit the corresponding entities uncondition–

ally. As the previous chapter of this thesis explains, IAM systems may additionally consolidate step–up and adaptive authentication mechanisms that trigger authentication challenges under particular circumstances (e.g., accessing high–risk resources and initiating connections from unexpected IP addresses). However, such deterministic approaches cannot prevent fraudulent activities that do not match the predefined risk scenarios. Step–up authentication enforces authentication challenges as soon as specific pre–configured events are detected, whereas adaptive authentication typically lacks the intelligence to detect threats beyond the organization's risk tolerance [47]. Continuous authentication, therefore, intervenes to address such limitations and further improve the security posture of organizations.

The available literature—which the author could obtain—does not make clear distinctions between the characteristics of adaptive and continuous authentication processes. There are IAM professionals who consider continuous authentication as an evolvement of adaptive authentication, while others prefer to use these terms interchangeably. Continuous authentication is essentially responsible for verifying identities periodically to ensure that their activities are legitimate [48]. Towards this purpose, there are technologies around analytics and AI that investigate user activity and make comparisons against pre–established behavioural patterns—this chapter provides additional information concerning these later on. In parallel, physiological (e.g., fingerprint, face, and iris recognition) and behavioural (e.g., keystroke, mouse, and touch dynamics) biometric traits can support the purposes of continuous authentication while offering convenience and distinctiveness [49]. However, as biometric–related processes are subject to attacks (e.g., impersonation and circumvention), research has suggested multimodal biometric authentication schemes for improving recognition accuracy and decreasing the likelihood of misuse [50]. Biometrics, alongside AI–powered technologies, are highly favourable for achieving continuous authentication due to their ease–of–use and frictionless approach to low–risk activities.

Figure 3.3 breaks down the fundamental components of continuous authentication. Firstly, the user provides their biometric traits and contributes to establishing their behavioural patterns. The continuous authentication process leverages biometrics and behavioural patterns and performs frequent checks in the background. Provided that the process does not detect any deviations and high–risk activity, the user can continue accessing the SP without interruption. Alternatively, continuous authentication triggers an authentication challenge to verify the user's identity.

As many organizations nowadays operate both on–premises and cloud infrastructures, continuous authentication becomes more complicated to configure. The challenges behind the real–time authentication and authorization involve the constant evaluation of devices and their security postures, the prompt attenuation and revocation of sessions, the appropriate enforcement of session–level controls, and the reciprocal

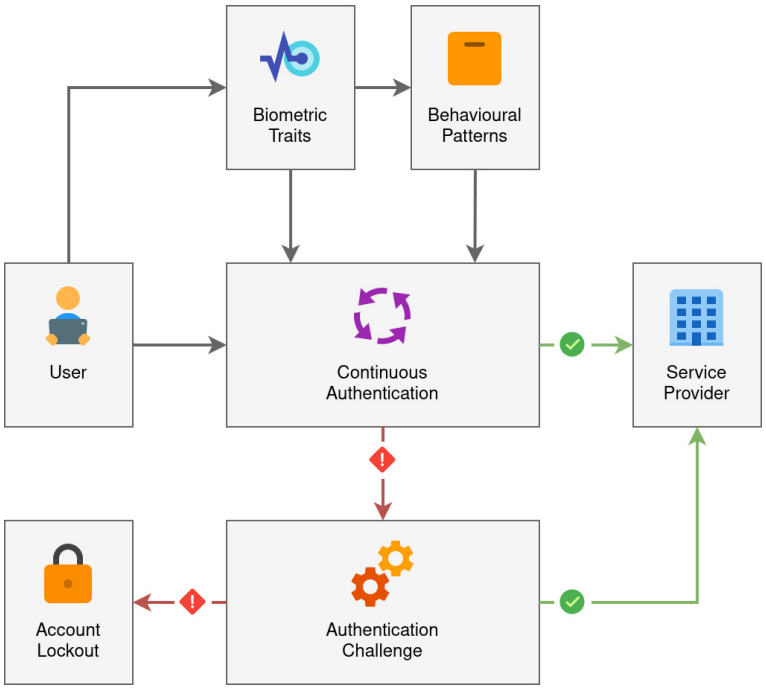

Figure 3.3: Continuous Authentication Flow

sharing of identity intelligence [51]. Organizations that address such challenges position themselves towards achieving ZTM that differs from standard perimeter–based security paradigms and goes hand–in–hand with continuous authentication. ZTM encourages performing real–time monitoring of applications and APIs, ensuring continuous authentication throughout each session, and triggering re–authentication as soon as high–risk or unusual activities are detected [52]. Later, this chapter further explores ZTM and its relationship with continuous authentication and other developments.

3.2.3 Passwordless Authentication

Password–based authentication is simple for end–users to operate, straightforward for developers to configure, and compatible with every platform and device. However, password maintenance practices require considerable effort and cannot always safeguard passwords against unwanted exposure (e.g., data breaches and phishing attempts). Even though organizations cannot progress to the complete phaseout of passwords right now, password–related constraints have motivated the development of infrastructures that practice modern techniques around provisioning and de–provisioning, adaptive and risk–based authentication, and strong encryption [53]. These establish

the foundation for the future of passwordless authentication.

Research exhibits that end–users are eager to choose passwordless authentication (i.e., using security devices) over password–based authentication but meanwhile express the following concerns [54]:

- The potential loss of security devices that undermines the recovery of accounts;
- The reusability of security devices across multiple platforms that increases the risk of massive loss of access;
- The concealment of security devices that is more difficult than memorizable passwords;
- The compatibility of security devices with end–user devices that is not guaranteed (e.g., lack of accessible USB ports); and
- The knowledge of end–users around security devices is inadequate, as they are most familiar with password–based authentication.

As far as the above–mentioned challenges are concerned, there are potential solutions such as attaching additional factors of authentication for backup purposes and increasing awareness around the advantages and constraints of security devices. Regardless, passwordless authentication does not involve security devices only. Biometrics (e.g., fingerprint identification, face recognition, and voice recognition) and authentication tokens (e.g., JWTs) constitute passwordless authentication, too.

Biometrics decrease the likelihood of identity theft, prevent the memorization of information, obstruct the guessing of authentication–related modalities, and diminish the sharing of biometric information [26]. If compromised, though, they increase the chance of abuse and render their replacement incredibly complicated if not impossible. Consequently, people often hesitate to provide and practice their biometrics for authentication purposes. Additionally, people with injuries or disabilities may face difficulties. Hence, it appears that biometrics (i.e., something–you–are) cannot displace the other two factors of authentication (i.e., something–you–know and something–you–have).

Token–based authentication indicates another example of passwordless authentication that renders standard password inputs obsolete. IdPs practice public–key cryptography, sign tokens, and share them with SPs whenever transferring identity and security–related information. The previous chapter of this thesis introduces FIM and presents SAML, OAuth, and OIDC that orchestrate the exchanging of authentication and authorization data. In particular, these protocols exercise SAML Assertions, OAuth Access Tokens, and JWTs, respectively. Furthermore, some organizations practise the concept of email–based passwordless authentication, also known as magic link authentication, in which the end–user receives an e–mail message, clicks on the link that contains an embedded token (e.g., JWT), and proceeds to the target SP without entering any password [55].

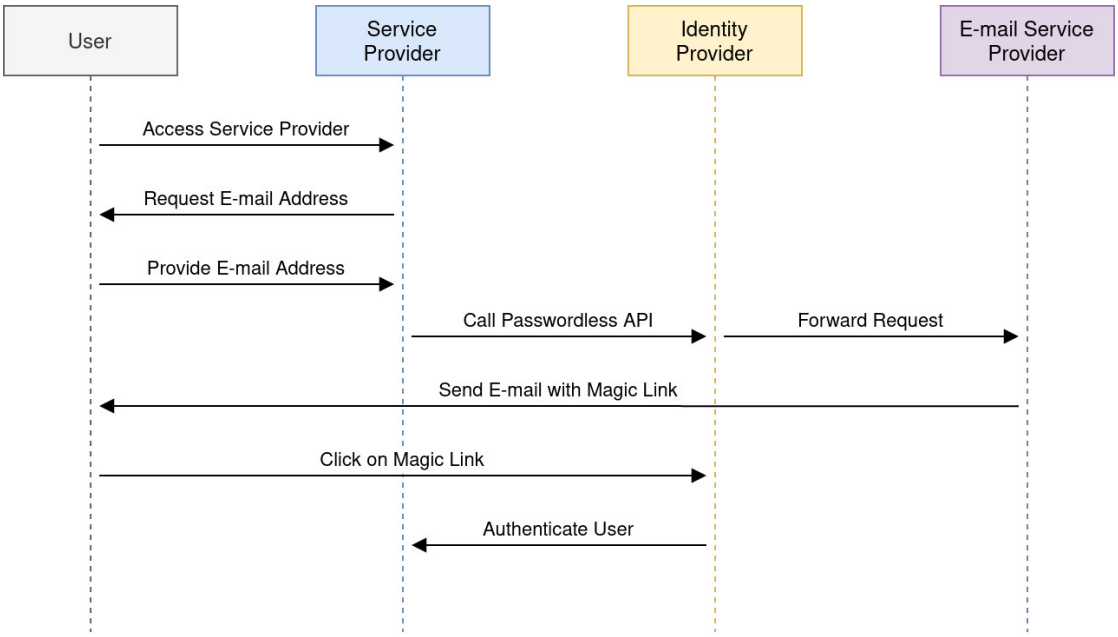

Figure 3.4: Magic Link Authentication Sequence — Adapted [56]

Figure 3.4 emphasizes an example sequence for conducting magic link authentication. In the beginning, the user accesses the SP and chooses to log-in. As soon as the service provider requests the user's e-mail address, the user submits their e-mail address. Then, the SP communicates with the IdP. The latter processes the request and, in turn, communicates with the e-mail SP. The e-mail SP sends an e-mail to the user containing the magic link. Finally, the user accesses the e-mail, clicks on the magic link, and proceeds with the authentication as arranged by the IdP.

3.2.4 Attribute-Based Access Control

The previous chapter of this thesis highlights MAC, DAC, and RBAC as well-established access control models. During the last decade, ABAC has gained increased popularity for its potential benefits to organizations. NIST regards ABAC as an access control model under which requests from subjects are granted or denied based on assigned attributes, applicable environment conditions, and policies related to those attributes and environment conditions [57].

As per ABAC, the authorization engine needs to take the following parameters into account whenever making access decisions [58]:

- The subject, which means the human or the non-human user that attempts to

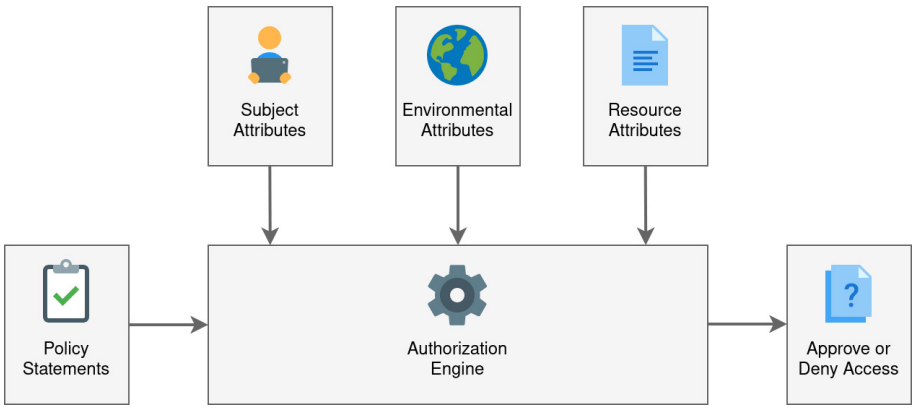

Figure 3.5: ABAC Flow — Adapted [59]

access resources and perform actions;
- The resource, which indicates the actual asset or object that the subject attempts to access;
- The action, which suggests what the subject attempts to accomplish with the resource (e.g., read, write, or delete); and
- The environment, which involves contextual factors around the access request (e.g., date and time, location, device identifier, communications protocol, and encryption standard).

The appropriate configuration and enforcement of ABAC presuppose the accurate assignment of attributes to identities. As discussed in the previous chapter, this commitment ordinarily applies to ILM that, in turn, acknowledges different JML scenarios. Apart from attributes, ABAC depends on predefined policies that correlate subjects, resources, actions, and environmental factors. Each organization defines the relevant policies and describes the scenarios in which entities request access to resources.

Figure 3.5 further elaborates on the components and structure of ABAC. The authorization engine considers subject attributes, environmental attributes, and resource attributes alongside the corresponding policy statements before determining whether to approve or deny access. Moreover, Figure 3.6 represents an example policy statement that incorporates two user attributes and one environmental attribute, specifies an object attribute, and designates an action permitted.

Organizations choose ABAC to accomplish granular access control and, in particular, fine–grained authorization that involves precise rules. Additionally, ABAC can co–exist with separate access control models such as RBAC for achieving coarse–grained authorization. Analyses have indicated that ABAC increases the overall requirements around attribute management due to its elasticity and comprehensiveness, so many

All entities that belong to the HR department, are managers, and connect from the office in Athens, are granted write access to contract documents.

Figure 3.6: ABAC Policy Statement

researchers have introduced hybrid ABAC models and frameworks to remediate such issues [60]. ABAC requires more effort in planning and implementation than RBAC but offers higher scalability and enhanced access security upon deployment [61].

The research community has developed several pure and hybrid approaches to ABAC during these years. Researchers have proposed an ABAC mechanism that features two–stage authorization and acknowledges both attribute–based and privacy–oriented policies [62]. Moreover, the advantageous characteristics of ABAC have contributed to suitable cloud–based access control approaches for the IoT domain and, specifically, intelligent transportation systems [63].

Attribute–Based Encryption (ABE) is often confused with ABAC, although both revolve around attributes. ABE furthers the long–established concept of Identity–Based Encryption (IBE) and provides asymmetric encryption in which the secret key of the user and the ciphertext depend on distinct attributes. Nonetheless, ABE can operate alongside ABAC. Academics have considered the involvement of ABAC and ABE whenever controlling access across cloud storage environments. Research has demonstrated that ABAC can support the management and enforcement of policies together with Advanced Encryption Standard (AES) protecting cloud data by the first encryption (thus ensuring faster performance) and ABE securing the symmetric encryption key [64].

3.2.5 Just–In–Time Access

JIT privileged access helps ensure that users obtain the appropriate privileges whenever necessary and for the minimum period required. It contributes to the enforcement of PoLP and supports organizations with their efforts in security. The JIT access process orchestrates the assignment of privileges for legitimate reasons and subsequently removes them as soon as the user completes the intended task or the predecided time window expires [65].

In regard to the academic landscape, this thesis cannot indicate any research directions towards JIT access. At the time of the writing, the available academic databases and search engines do not return any matching results. This constraint forces the author to draw relevant information from PAM vendors entirely.

Figure 3.7 shows an example scenario for JIT access requesters. The user first submits their request to obtain privileged access. Next, the PAM system examines the

user's request and, as long as no information is missing, notifies the approver who is responsible for handling such requests. The approver then reviews the user's request and submits their decision. If the request is approved, the PAM system initiates the provisioning process and the corresponding SPs update the user's accounts as necessary. Lastly, the PAM system notifies the user regarding the outcome of their request. As anticipated, this specific scenario describes the procedure for requesting JIT access exclusively. It does not involve the de–provisioning mechanism and the subsequent removal of the assigned privileges.

Any form of manual intervention can nevertheless impair the frictionless user experience and create additional responsibilities for administrators. Thus, organizations opt for automating their processes and setting up policies for controlling JIT access. Upon configuration, the PAM system can analyze several commands and applications to detect compromise, examine attempts to access sensitive resources, validate the statuses of user sessions, search for illegitimate modifications of resources, discover attempts for lateral movement through the network, and monitor the manipulation of user accounts and data sets [66].

Depending on the exact approach, JIT access provisioning may enable the elevation of privileges for specific periods but often cannot anticipate the risks associated with compromised accounts. If users receive additional permissions through JIT access for prolonged periods, attackers have an opportunity for exploitation. Hence, Zero Standing Privileges (ZSP) has emerged as the JIT access strategy that decreases the amount of time for granting permissions, enables the precise scoping of allowed activities, and eliminates the risk of users having standing privileges [67]. ZSP reinforces the broader PAM posture and aids organizations in meeting their security requirements besides gaining operational benefits [68].

Apart from the benefits mentioned earlier, time–limited access conforms with the expectations of PoLP and aids the implementation of ZTM. It helps reduce insider threats by narrowing down access permissions, limits the scope of damage upon credential compromise, and supports compliance requirements thanks to its auditing capabilities [69]. JIT access draws the security perimeter around identities rather than trusted systems and makes the transition to ZTM more straightforward.

3.2.6 Zero–Trust Model

ZTM has become widespread amongst information security professionals and has carried the catchphrase "never trust, always verify". Although often referred to as the Zero Trust Architecture (ZTA), there are slight differences. According to NIST, ZTM symbolizes the cybersecurity paradigm that focuses on protecting resources and continuously evaluates trust, least privilege per–request access decisions, whilst ZTA constitutes

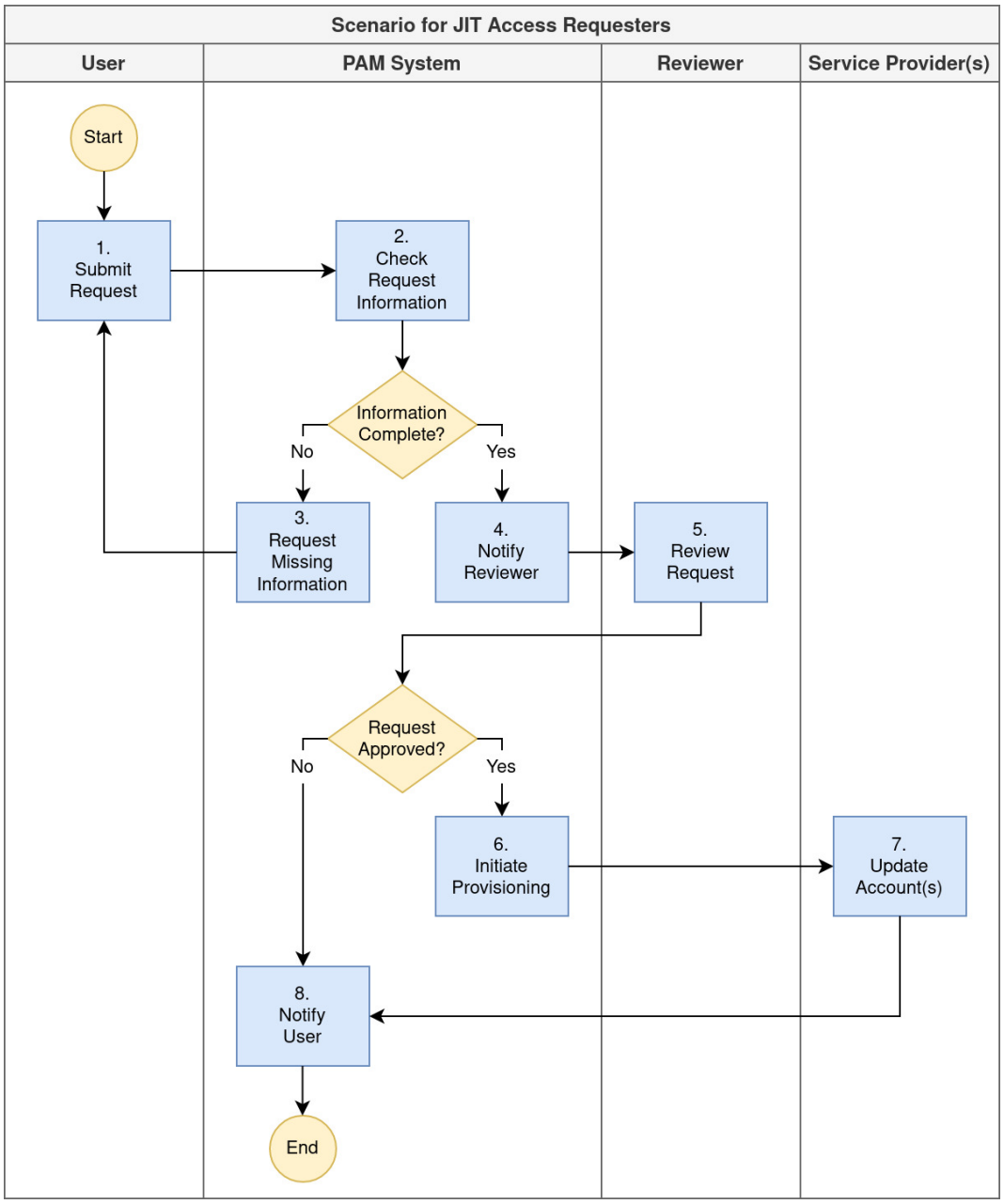

Figure 3.7: Scenario for JIT Access Requesters

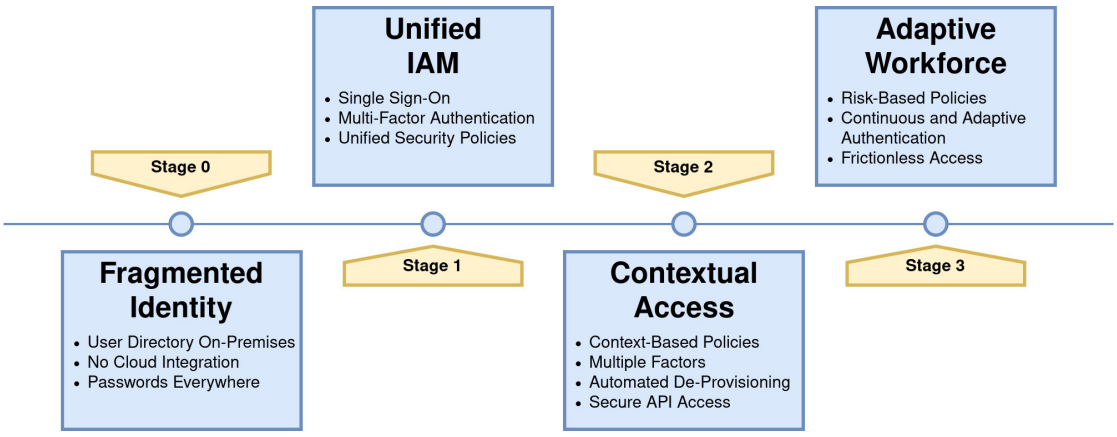

Figure 3.8: Zero–Trust Maturity Model — Adapted [72]

an end–to–end approach (i.e., cybersecurity plan) that spans across identities, credentials, access management, operations, endpoints, hosting environments, and the underlying infrastructure [70].

ZTM practically corresponds to tight IAM–related measures. There are four key conditions before implementing ZTM that require organizations to [71]:

- Draw attention to identities while acknowledging there are no longer trusted security perimeters (e.g., firewalls) and that every human and non–human user is bound to continuous authentication;
- Enforce step–up and adaptive authentication for the static and dynamic assessment of risks and leverage MFA as necessary;
- Replace passwords with signed assertions or tokens whenever possible and thus reduce the traditional attack vectors; and
- Define and manage centralized policies for both on–premises and cloud environments to prevent inconsistencies, avoid weaknesses, and decrease the administrative burden.

Regarding cloud computing environments, research indicates that ZTM requires identifying sensitive data (i.e., personal data, financial data, and confidential data), mapping the flows of sensitive data, ensuring the continuous supervision of user and device authorization, enforcing least privilege access, safeguarding critical resources, reinforcing application security, and monitoring security with analytics [73]. Meanwhile, PoLP is necessary to shrink the broader attack surface that expands with the accelerated adoption of cloud computing, as attackers can escalate excess privileges, perform data exfiltrations, disrupt critical applications, and even overtake entire cloud deployments [74]. Therefore, organizations that operate cloud or hybrid environments need

to consider the proper enforcement of PoLP before achieving ZTM.

Research also suggests that under ZTM, the calculation of the risk score—that ultimately helps the IAM system determine whether or not to grant access—should consider the classification of data, analyze the configuration and functioning of endpoint devices, monitor security-related user behaviour, and acknowledge security policies [75]. For this purpose, ZTM encourages the use of modern technologies such as machine learning and analytics that support the evaluation of the identity context (e.g., devices and networks), the detection of anomalous activity, the enforcement of policies, and the suggestion of access-related decisions [76].

Figure 3.8 explains the typical maturity levels of organizations that wish to adopt ZTM. The fragmentation of identities across unintegrated systems can undermine the experience for end-users, increase the workload for administrators, and expand the possibility for successful exploitations by malicious attackers. Instead, the unification of IAM combines SSO, MFA, and comprehensive security policies to address the beforementioned challenges to an extent. Then, the establishment of context-based policies, the adoption of additional authentication factors, the configuration of automated de-provisioning, and the implementation of secure API access defend the organization against more sophisticated attacks while streamlining IAM operations. Eventually, the adaptation of risk-based policies, the deployment of continuous and adaptive authentication processes, and the enabling of frictionless access control enhance security, increase agility, and provide further confidence to the organization and the end-users.

3.2.7 Identity Analytics

Analytics is the practice of processing large amounts of data, identifying meaningful patterns, and providing insight into performance. Organizations can integrate analytics into their IAM program, obtain increased visibility over identities, and identify potential weaknesses such as inappropriate access rights, excess privileges, and SoD conflicts. Upon the identification of gaps, organizations can make the necessary adjustments and improve their security posture significantly.

It appears that the popular academic search engines and databases—which the author could consult throughout the preparation of this thesis—do not contribute with relevant material around identity analytics. This observation probably means that the academic community has not yet prioritized this research area. Contrarily, industry professionals and IAM vendors demonstrate substantial research and development. As a consequence, this master's thesis aligns with industry perspectives.

The risk of excessive access, the regulatory obligations, and the improvement of operational efficiency are three factors that drive the adoption of identity analytics [77]. As long as organizations cannot obtain insights into the assigned access rights, the

risk of excessive access remains tough to mitigate. Regarding regulatory compliance, organizations often struggle with monitoring existing policies and promptly detecting any violations. Thirdly, heterogeneous digital environments increase the complexity of monitoring identities and create an administrative burden. Identity analytics addresses these challenges and guides organizations towards making more reliable decisions.

Identity analytics contributes to the recent paradigm shift in IAM, according to which organizations should focus on predicting rather than reacting. In this direction, there are three categories of statistical behaviour concerning digital identities [78]:

- Data clustering, indicating the ability of administrators to detect patterns amongst users (e.g., the identification of groups with similar or conflicting access rights);
- Weighted search, meaning the functionality that analyzes user roles alongside user activity and guides access requests (e.g., the auto–suggestions regarding access rights); and
- Automated remediation, implying the detection of anomalies and the subsequent actions for their correction (e.g., the discovery of users whose access deviates from the rest of their group).

Figure 3.9 resembles an identity cluster analysis and, in particular, k–means clustering in which identities form clusters according to their access roles. The analytics process then flags the remaining individual identities that deviate from ones belonging to the three clusters. Depending on the exact arrangement of the IAM or IGA program, the responsible administrator may intervene to revoke excessive access rights from the flagged identities or proceed with the appropriate course of action.

As the previous chapter discusses, IGA systems prioritize the detection of potential risks around security and compliance. Although identity analytics resembles the purposes of IGA, such functionality can also appear under conventional IAM systems. Regardless of whether organizations integrate analytics with an IAM or IGA system, the initiating configuration and deployment phases require thoughtful planning and significant commitment. Analyses demonstrate that those who prioritize analytics—when investing in IAM and IGA—maximize the return on their investments [79]. Hence, analytics processes are influential segments of modern IAM and IGA programs.

3.2.8 Identity and Artificial Intelligence

The previous subsection approaches the essential characteristics that comprise identity analytics and outlines their involvement in modern IAM and IGA programs. It stands to reason that such functionality often intertwines with AI, Machine Learning (ML), and Deep Learning (DL). The continuous improvements in IAM and IGA have prompted

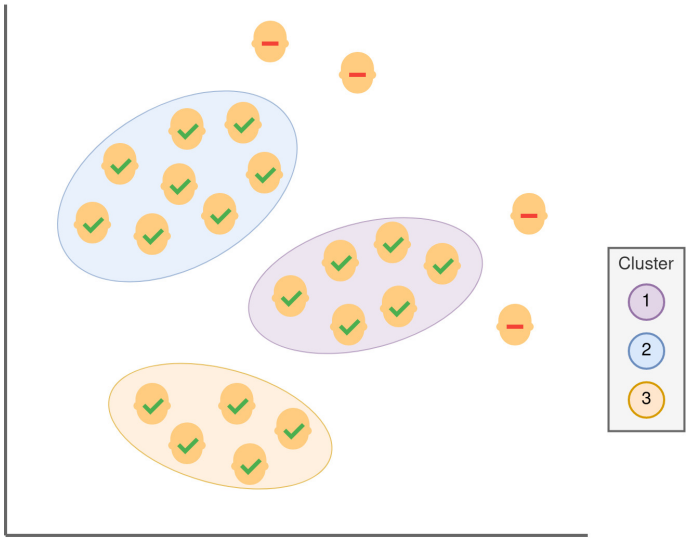

Figure 3.9: Identity Cluster Analysis

the emergence of unique terms including, but not limited to, AI–Driven Identity, AI–Powered Identity, Autonomous Identity, Predictive Identity, and Smart Identity. Typically, the few IAM and IGA vendors that have coined the before–mentioned terms are the ones practising them. Meanwhile, other vendors prefer to highlight the underlying technologies, such as AI and ML, used within their products.

Admittedly, some academics and industry experts declare that the use of sophisticated algorithms does not necessarily fall under the AI domain. This master's thesis does not investigate this matter further and—for the sake of simplicity—assumes that such processes indeed constitute applications of AI. Furthermore, at the time of writing, the academic literature—which the author of this thesis could access—does not reference identity and AI. This observation is considerably similar to the one regarding identity analytics. Accordingly, this thesis is bound to consider content from IAM and IGA vendors and industry professionals entirely.

AI–driven automation furthers the contributions of identity analytics and allows for auto–suggestions whenever addressing frequent challenges. Specifically, it can collect intelligence and present insights regarding an IAM or IGA program, streamline the assignment and maintenance of roles according to the particular needs of the organization, and provide automated recommendations during access requests and certifications [80]. Automation, therefore, decreases the manual intervention required during repetitive access requests and empowers managers to concentrate on unusual or high–risk requests [81].

Figure 3.10 illustrates the AI–driven decision cycle regarding identities. At first, the

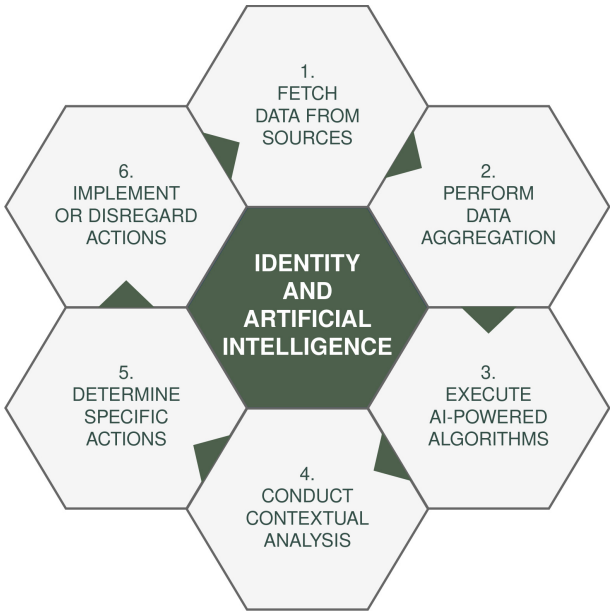

Figure 3.10: AI–Driven Identity Decision Cycle — Adapted [82]

IAM or IGA system fetches data from multiple databases (e.g., authoritative sources) and proceeds with the necessary correlations. The system then applies its AI–powered algorithms to the aggregated data and searches for any risks associated with identities. Following the identification of potential risks, the system performs contextual analysis and determines the appropriate courses of action. Depending on the design of the IAM or IGA program, the system may either implement its recommendations unattended or lead to an escalation and request manual intervention.

Moreover, AI–related technologies can significantly contribute to increasing the maturity of ZTM. Upon generating behavioural profiles, they distinguish between ordinary and anomalous behaviour and enforce dynamic policies that do not require manual intervention. In essence, they continuously evaluate users against the predetermined behavioural patterns and automatically take action (e.g., approve access, deny access, remove privileges, terminate sessions, or disable accounts) depending on the detected levels of risk [83]. While AI–powered IAM and IGA systems emphasize the enforcement of security controls dynamically, they cannot eradicate conventional rule–based and context–based policies.

The direction towards next–generation IAM systems introduces AI technologies into the authentication–related processes and researches viable approaches for delivering an enhanced authentication experience. As the previous chapter of this thesis mentions, password–based authentication associates with common attack vectors. At the

same time, however, step–up and adaptive authentication processes create an additional burden for end–users. This controversy drives potential improvements in IAM systems that include dynamic risk detection capabilities around authentication [84]. The intention is to avoid imposing follow–up authentication challenges upon end–users if not deemed necessary.

3.3 Chapter Summary

The third chapter of this master's thesis examines eight emerging approaches to IAM and presents their advantages alongside their potential disadvantages. The following paragraphs summarize the fundamental characteristics of each of these approaches. In addition, Table 3.1 helps visualize the summary of this chapter and consolidates the corresponding bibliographic citations.

Blockchain disrupts the field of IAM and introduces user–centric IdM alongside the existing network–centric and application–centric approaches. Thanks to its tamper–resistant design, blockchain supports organizations with their efforts in information security and data protection. Furthermore, it increases control, improves transparency, fosters selective anonymity, and enables trust–based IdM. However, blockchain also imposes some challenges on GDPR compliance and thus cannot store personal data. Nevertheless, academics have performed research on GDPR compliance. They have also considered distributed ledgers in IAM for IoT.

Continuous authentication allows for the non–stop verification of identities and complements the well–established step–up and adaptive authentication processes. It leverages analytics, AI–powered technologies, and multimodal biometrics to balance the security specifications that organizations require and the convenience that end–users seek. Furthermore, continuous authentication addresses the requirements for achieving zero–trust but requires considerable commitment from organizations.

Passwordless authentication goes hand–in–hand with the advancements in IAM–related techniques such as provisioning and de–provisioning, adaptive and risk–based authentication, and strong encryption. It eliminates the common risks associated with password–based authentication while providing the level of confidence necessary for end–user adoption. This thesis does not indicate any significant challenges related to passwordless authentication.

ABAC reinforces granular access control and relies upon predefined policy statements that incorporate subjects, resources, actions, and environmental factors. In particular, ABAC focuses on fine–grained control and can work together with other models such as RBAC for enabling coarse–grained control. ABAC offers higher scalability but increases the requirements around attribute management. This contradiction leads to

more efforts during the planning and implementation phases. Academics and industry professionals have researched hybrid ABAC models to remediate these challenges and offer additional functionality.

JIT access arranges the temporary assignment of privileges to users and ensures their prompt removal upon the completion of the intended task or the expiration of the predefined task window. Organizations can either configure manual mechanisms for requesting access, where users submit their requests and human reviewers provide their decisions, or automate their JIT access workflows. This thesis cannot find any academic research on JIT access but draws relevant information from PAM vendors instead. JIT processes aid PAM systems in fulfilling their duties and ensuring the security of privileged accounts across several environments. However, as they sometimes cannot anticipate the risks around standing privileges, organizations begin to adopt ZSP strategies. Last but not least, time–limited access supports the enforcement of PoLP and makes the achievement of ZTM more straightforward.

The ZTM carries the motto ”never trust, always verify” and establishes perimeterless security. It leverages modern IAM–related technologies to protect resources, evaluate trust, and enforce least privilege access decisions for each request. In particular, ZTM enforces PoLP to the greatest extent and prevents the escalation of excess privileges, the execution of data exfiltrations, the disruption of critical applications, and even the overtaking of entire deployments. However, it necessitates tight IAM–related measures and may require organizations to perform specific improvements around the evaluation of the identity context (e.g., devices and networks), the detection of anomalous activity, the execution of policies, and the enforcement of access–related decisions.

Identity analytics helps organizations obtain increased visibility over identities and identify potential weaknesses such as inappropriate access rights, excess privileges, and SoD conflicts. Besides, it supports regulatory compliance and provides predictive capabilities to organizations so that their focus shifts from reacting to predicting. This thesis indicates that industry professionals and IAM vendors demonstrate substantial research and development while academics do not contribute with relevant material. Although organizations need to make considerable commitments before establishing identity analytics, they can achieve significant returns on their investments.

AI–powered technologies further increase the influence of identity analytics. They provide automated recommendations (e.g., during identity certifications and access requests), minimize manual intervention concerning repetitive activities, and decrease the administrative burden associated with running an IAM program. As they analyze identities against predetermined behavioural patterns, they help prevent fraudulent activity and point to potential IAM–related improvements. This direction towards the next–generation IAM systems encourages particular improvements on authentication (i.e., continuous authentication that complements step–up and adaptive authentication) and

supports the establishment of the ZTM. This thesis acknowledges that the available academic literature does not provide any relevant content regarding the relationship between identity and AI.

Table 3.1: Emerging Approaches — Summary

Category	Name	Advantages	Disadvantages
Administration	Identity and Blockchain	Supports Security and Data Protection Efforts [40], Fosters Research on GDPR Compliance [42] and IoT [45], Increases Control and Improves Transparency [43], Supports Selective Anonymity and Enables Trust–Based IdM [44]	Imposes Challenges on GDPR Compliance [41]
Authentication	Continuous Authentication	Complements Step–Up and Adaptive Authentication Processes [47], Leverages Analytics, AI–Powered Technologies and Multimodal Biometrics [49] [50], Addresses Zero Trust Approach [52]	Requires Significant Commitment [51]
	Passwordless Authentication	Advances IAM–Related Techniques [53], Encourages End–User Adoption [54]	None Examined
Authorization	Attribute–Based Access Control	Establishes Granular Access Control [58], Provides Higher Scalability [61], Fosters Research on Hybrid Models [62] [63] [64]	Increases Complexitity and Requires Considerable Investment [60]

	Just–In–Time Access	Orchestrates Privilege Assignments [65], Improves PAM Capablities [66], Eliminates Standling Privileges [67], Generates Operational Benefits [68]	None Examined
	Zero–Trust Model	Establishes Perimeterless Security [75], Leverages Modern IAM–Related Technologies [76]	Requires Strict IAM–Related Measures [71] [73] [74]
Governance	Identity Analytics	Addresses Prioritized Risks and Supports Regulatory Compliance [77], Provides Predictive Capabilities [78], Maximizes Return on Investments [79]	Requires Considerable Commitment [79]
	Identity and Artificial Intelligence	Provides Automated Recommendations [80], Decreases Administrative Burden [81], Leverages Behavioural Patterns [83], Drives Potential IAM–Related Improvements [84]	None Examined

4 Adoption and Transformation

4.1 EU Policies and Initiatives

Currently, there is no comprehensive information available to the public regarding the particular IAM concepts, principles, mechanisms, and technologies that the various e-government services across the EU embrace. The scope of this master's thesis does not involve any relevant case study analyses. Alternatively, the author intends to examine the broader direction of the EU towards information security, privacy, and data protection. In particular, this chapter reflects upon the EU's strategy—that the European Commission (EC) develops and translates into policies and initiatives—and correlates them with the eight emerging approaches to IAM of the previous chapter.

The first subsection mentions the ongoing revision of the EU regulation for Electronic Identification, Authentication and Trust Services (eIDAS). Then, the second subsection features the development of the European Self-Sovereign Identity Framework (ESSIF). Moreover, the third subsection considers the upcoming revision of the EU directive for Network and Information Security (NIS). Last but not least, the fourth subsection explores the Artificial Intelligence Act (AIA) that comprises the recent proposal for an EU regulation laying down harmonized rules on AI.

4.1.1 eIDAS Regulation Revision

The eIDAS Regulation, namely Regulation (EU) 910/2014, intends to harmonize and facilitate secure cross-border transactions in the EU. The technological advances of the previous decades compelled the replacement of the EU's former directive on the use of electronic signatures (i.e., Directive 1999/93/EC). In contrast to EU directives that compel their transposition into national legislation [85], eIDAS as an EU regulation is legally binding and directly applicable in every member state [86]. This distinction presumably indicates that the legislators emphasize the consistent implementation of the eIDAS specification across the entire EU.

eIDAS establishes the foundation for building trust relationships and promoting the exchange of identity information among EU member states. The idea is that member states operate eIDAS nodes that act as the point-of-contact for IdPs and SPs. Each node incorporates two components for actualizing its corresponding operation modes:

a) the connector for assisting SPs and requesting cross–border authentication and b) the proxy server for supporting IdPs and providing cross–border authentication. Essentially, eIDAS nodes forward SAML authentication requests and SAML assertions. Regardless, SPs and IdPs might implement different authentication and authorization mechanisms as long as they can translate SAML statements [87].

The introduction of eIDAS enables people and businesses to use their national electronic identification schemes whenever accessing services provided by other EU member states. It leads to an internal market for trust services that covers electronic signatures, electronic seals, electronic timestamps, electronic registered delivery services, and qualified website authentication certificates. In particular, eIDAS ensures that these trust services have the same legal status as traditional paper–based processes and guarantees they work across borders [88].

The EC launched a public consultation on the revision of eIDAS to collect opinions from multiple stakeholders and citizens and determine the current situation regarding the regulation [89]. The intention was to obtain insights into improving efficiency, fostering adoption, and acknowledging the latest technological requirements. Before the public consultation, the Inception Impact Assessment (IIA) informed citizens as well as relevant stakeholders and highlighted the following challenges [90]:

- 15 out of 27 member states offer eIDAS to their citizens, implying that the current situation corresponds to inconsistencies and inequalities across the EU;
- eIDAS encourages member states to make their national electronic identification schemes compatible with private SPs, although the overall adoption and implementation rates are significantly low;
- Private SPs sometimes offer identity federation with third parties (e.g., social networking platforms), although such schemes operate in an unregulated environment and citizens often raise their concerns about privacy and data protection;
- The third–party identity federation schemes do not necessarily correlate to verifiable physical identities, meaning that they increase the difficulty to mitigate potential threats related to fraud (e.g., identity theft) and information security; and
- The current state of eIDAS does not reflect modern technologies (e.g., AI, IoT, analytics, and biometrics) and does not address the increasing expectations of users about enhanced anonymity.

Moreover, the European Network and Information Security Agency (ENISA) published a report that indicated the following tendencies in the field of digital identity [91]:

- The expanding penetration of mobile devices in the EU reinforces the concept of mobile identity services and the establishment of mobile–based identification schemes by the member states;

- In the context of authentication, behavioural biometric traits and multimodal biometric systems lead to significant traction and improvements in accuracy, reliability, transparency, and security;
- Besides public sector organizations, private sector organizations boost their participation in the digital identity ecosystem and provide corresponding solutions to their customers and other entities;
- The increasing expectations of citizens, as well as the privacy and data protection requirements in the EU, impact the management of digital identities; and
- The evolution of disruptive technologies such as distributed ledgers—in connection to the persistent concerns about privacy and data protection—encourage the development of SSI approaches.

The IIA declared that the dramatic increase in the use of innovative technologies and the emergence of several organizations with significant market power—that might act as digital identity gatekeepers— drive the revision of regulation. The main objective is to build an updated and future-proof framework for IdM that covers the identification and authentication processes alongside the provisioning of attributes, credentials and attestations. The IIA then proposed three policy options with different degrees of legislative intervention and elaborated on the expected levels of impact on the economy, the society, the environment, the fundamental rights of people, and the administrative burden of public and private SPs. Those who participated in the subsequent public consultation process had the opportunity to express their views, data, and evidence and assist the EC with choosing the regulatory option.

The revision of eIDAS is significant in modernizing the framework for digital identity in Europe and rendering it future-proof. Nowadays, as people demand the presence of proper safeguards for privacy and data protection, the EC can use this opportunity to align eIDAS with modern technological advances such as blockchain for IdM that can actualize the vision of the SSI model.

4.1.2 ESSIF Development

In parallel to the revision of eIDAS, the EC investigates the applicability of SSI to several use-cases. Specifically, the SSI approach shows considerable promise in issuing and verifying different categories of digital credentials whilst enabling citizens to maintain control of their data.

Thirty countries—both within and outside the EU—form the European Blockchain Partnership (EBP) and operate the European Blockchain Services Infrastructure (EBSI). EBSI intends to support the delivery of cross-border digital public services and oversee the utilization of stringent data security measures. Alongside EBSI, EBP promotes

the development of ESSIF to expedite the cross–border adoption of the SSI approach, foster the interoperability amongst national SSI schemes, ensure the alignment with eIDAS, and build an identity layer within EBSI. The initial version of ESSIF supports limited functionality and essentially serves demonstration purposes [92], as the current version of EBSI does not run in production. Nevertheless, the technical specification sets the direction towards expanding the scope and the characteristics of ESSIF.

ESSIF demonstrates the potential for streamlining e–government and e–commerce processes and enhancing IAM. The vision that guides the development of the framework derives from the following considerations [93]:

- The conventional IdM practices are not user–centric, implying that people have little control over the exposure of their personal data and identity attributes to SPs;
- There are not enough trusted and easy–to–use mechanisms for controlling the distribution of personal data, so people often struggle with exercising their rights to privacy and data protection;
- The diverse specifications of e–government information systems and the subsequent obstacles to achieving interoperability make it complicated for SPs to retrieve up–to–date data and maintain their quality; and
- The member states are somewhat reluctant to invest in specialized hardware and software combinations for assisting their citizens with attestations.

The EU funds the ESSIF–LAB to facilitate the development, integration, and adoption of SSI technologies [94]. The initiative brings together experts from different disciplines and intends to support integrating SSI technologies with market propositions and accelerating their widespread adoption. Furthermore, the lab contributes to the design, maintenance, validation, and documentation of the framework.

As for the relationship between ESSIF and eIDAS, the EC intends to make eIDAS available as a trust framework in the SSI ecosystem. Therefore, the EC commits to developing the eIDAS bridge as part of ESSIF to ensure the legal validity of electronic documents and provide cross–border trust services. The previous chapter includes Figure 3.2 that illustrates how the issuer, the user, and the verifier can interact with the distributed ledger. Contrarily, Figure 3.2 presents an adjustment of the SSI approach that involves eIDAS bridges. It is noteworthy that the eIDAS bridge is not one horizontal component [95], as each issuer, user, and verifier can connect to different eIDAS bridges. In essence, eIDAS bridges feature two operation modes: a) they assist issuers with signing the verifiable credentials, and b) they support verifiers with assessing the trustworthiness of the verifiable credentials [96]. The integration between ESSIF and eIDAS enables the conversion of decentralized identifiers into verifiable credentials that assert the claims made by issuers about users.

ESSIF and the revision of eIDAS are the essential steps towards establishing the

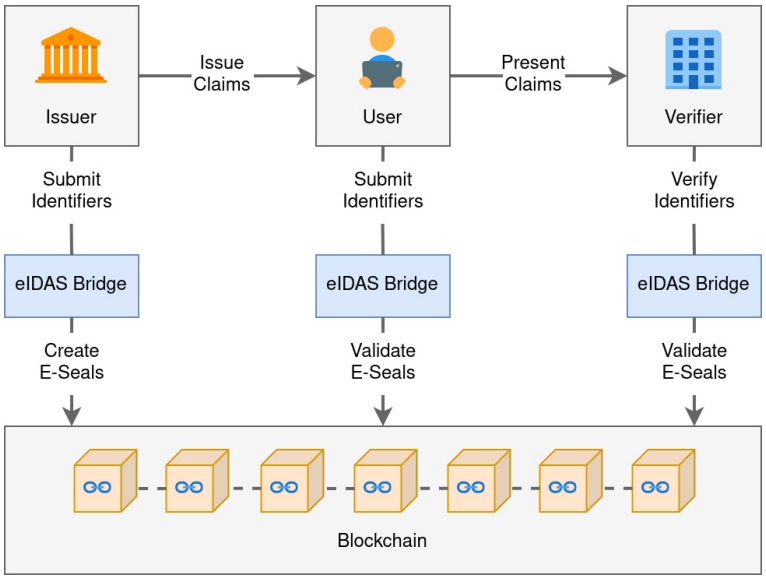

Figure 4.1: Self–Sovereign Identity Architecture with eIDAS Bridges

SSI model in the EU and capitalizing on the potential of EBSI to provide state of the art services regarding digital identity. Blockchain offers innovative perspectives on IdM and contributes to the needs of users, public and private sector organizations. It indicates the potential for a paradigm shift in IdM and IAM over the next few years.

4.1.3 NIS Directive Revision

The NIS Directive, namely Directive (EU) 2016/1148, guides the EU member states towards strengthening the security of their network and information systems. This legislative act concentrates on the security posture of operators of essential services (e.g., energy, transport, finance, and healthcare) and digital service providers (i.e., search engines, cloud computing services, and online marketplaces) [97]. Aside from assembling Computer Security Incident Response Teams (CSIRTs) and designating national authorities for NIS, the EU member states also participate in the NIS Cooperation Group that fosters their strategic cooperation, promotes the exchange of information, and supports the alignment of the national implementations.

While the EC acknowledged that the NIS Directive makes an enormous contribution to develop the cybersecurity capabilities and improve the protection of network and information systems across the entire EU, the IIA stated the following challenges [98]:

- The EU member states differentiate their approaches regarding the adoption of the directive, meaning there are currently important inconsistencies that cause

the fragmentation of the regulatory landscape;
- There are operators of essentials services and digital service providers with a presence in multiple EU member states that feel overwhelmed with the diverse security requirements and incident reporting procedures;
- The digital transformation—that accelerates due to the coronavirus pandemic—causes the expansion of the threat landscape and indicates the need for state of the art security measures.

The IIA stressed the negative impact of the fragmented approach to cybersecurity and highlighted the need for a state of the art response that considers the current cybersecurity requirements. Furthermore, it suggested four policy options that correspond to non–legislative measures and potential regulatory interventions. The IIA continued with assessing the expected levels of impact on the economy, the society, the environment, the fundamental rights of people, and the administrative burden of relevant entities. Following the public consultation process that collected feedback from organizations and individuals, the EC proposed a revised directive.

The revision extends the scope of the existing directive, eliminates the differentiation between operators of essential services and digital service providers, requires an approach to risk management and increases the overall requirements for organizations, strengthens the security expectations for supply chains, introduces stricter enforcement requirements for national authorities, and fosters the cooperation among member state authorities [99]. Moreover, the proposal emphasizes the public sector domain as part of its expanded scope, supports the coordinated disclosure of new vulnerabilities, imposes accountability obligations on organizations concerning their information security and risk management responsibilities, and refines the incident reporting process [100].

Furthermore, ENISA analyzed the NIS investments of 251 organizations across five EU member states and presented the following observations concerning the relationship between the NIS Directive and IAM [101]:

- Many organizations increase their involvement in managing the remote privileged and non–privileged access of their users;
- The progressive transition to cloud computing services requires identity as well as contextual approaches to information security and causes the IAM segment—that also involves IGA and PAM—to continue expanding;
- The relevant activities—that organizations undertake—often include provisioning, password management, directory integration, identity administration, 2FA or MFA, token–based authentication, PKI, PAM, FIM, SSO, and IGA; and
- Unauthorized access from compromised identities and credentials threatens organizations, so the enforcement of 2FA or MFA and PAM is necessary to improve the security posture and align with the expectations of NIS.

The increasing cybersecurity challenges and the expanding threat landscape highlight the importance of an updated legislative act. The revision of the NIS Directive corresponds to further expectations around information security and risk management. Meanwhile, the configuration and deployment of IAM concepts, principles, mechanisms, and technologies lead to improving the security posture of public and private sector organizations. As the previous chapter explains, the emerging approaches to IAM can assist organizations with withstanding sophisticated attacks and complying with regulatory obligations.

4.1.4 AI Regulation Proposal

The progression of AI unleashes numerous opportunities for public and private sector organizations. As the previous chapter of this master's thesis explains, analytics processes and AI-powered algorithms aid the purposes of IAM, IGA, and PAM programs, too. However, the improper configuration and utilization of such capabilities might impact the fundamental rights of individuals and result in undesirable outcomes. Hence, the EC introduces the AIA as the first legal framework on AI [102]. The latest proposal for a regulation addresses the risks relating to AI and meanwhile encourages the adoption, investment, and innovation revolving around AI.

Earlier, the IIA recognized that AI technologies make predictions, optimize operations, allocate resources, and personalize service delivery. These capabilities allow for multiple economic, societal, and environmental benefits. Although, the IIA mentioned the following problems that require immediate intervention [103]:

- AI applications may cause material and immaterial harm such as jeopardizing the health and safety of individuals and imposing implications on the rights and freedoms of individuals;
- The harm—that AI applications might cause—often occurs due to defects in the overall design, the use of low quality or biased data, or flaws in the machine learning capabilities;
- The existing legislation does not provide an adequate level of protection against several challenges associated with AI, thereby obstructing the protection of the fundamental rights of individuals;
- The frequent lack of transparency as well as the technological complexity regarding AI applications (i.e., black-box effect) impair the appropriate enforcement of existing EU legislation; and
- AI-powered products and services usually cause legal uncertainty for organizations and impose challenges on market surveillance and supervisory authorities;

Furthermore, the IIA emphasized the need to create an ecosystem of trust around

AI and ensure the development and use of lawful and trustworthy AI applications. It proposed four preliminary policy options with different levels of intervention. The IIA proceeded with an early assessment of the impact on the economy, the society, the environment, the fundamental rights of individuals, and the administrative burden of relevant entities. In addition, the public consultation gathered opinions on the promotion of excellence across the AI domain, the implications of AI technologies on safety and liability, and the approach of the imminent regulatory intervention.

At the time of writing this master's thesis, the proposed regulation concerns: a) providers that operate AI systems in the EU, b) users of AI systems located in the EU, and c) providers and users of AI systems that are located in a third country where the output produced by AI systems is used in the EU [104]. The proposal introduces a risk–based approach and establishes the following classifications:

- If the risk is minimal, the AIA requires no further intervention;
- If the risk is limited, the AIA imposes transparency obligations and empowers users to make informed decisions;
- If the risk is high, the AIA expects the adherence of the systems to strict requirements before their acceptance; or
- If the risk is unacceptable, the AIA prohibits the use of the systems that threaten the safety, livelihoods, and rights of people.

The proposed regulation might be subject to adjustments prior to adoption. Nevertheless, it seems that the AIA may influence identity analytics and, generally, the AI–powered capabilities of modern IAM, IGA, and PAM systems in the near future.

4.2 Chapter Summary

The fourth chapter of this master's thesis looks into the EU strategy and associates some of the current policies and initiatives with the emerging approaches to IAM. In particular, it considers the eIDAS Regulation, the ESSIF, the NIS Directive, and the AIA. The following paragraphs summarize the latest developments in each of these. Moreover, Table 4.1 provides an alternative overview of the contents of this chapter.

The eIDAS Regulation arranges and facilitates secure cross–border transactions in the EU. It allows people and businesses to use their national electronic identification schemes whenever accessing services provided by other EU member states. In essence, member states operate eIDAS nodes that assist SPs with requesting cross–border authentication and support IdPs with providing cross–border authentication. eIDAS ensures that digital credentials have the same legal status as their paper–based

equivalents. Admittedly, the low adoption of eIDAS from member states leads to inconsistencies and inequalities across the EU. In addition, third–party identity federation schemes operate in an unregulated environment. At this moment, eIDAS does not reflect modern technological accomplishments and cannot support the users' expectations for enhanced privacy either. Therefore, the upcoming revision of eIDAS aims to address the present challenges and establish an updated framework for IdM that also acknowledges the SSI approach.

ESSIF is the framework for achieving user–centric IdM across the EU and accomplishing interoperability amongst the national SSI schemes. EBSI intends to provide decentralized digital identity services using ESSIF, although its current version supports specific use–cases. Currently, the conventional IdM practices often impose challenges on privacy and data protection. Moreover, there are persistent barriers to achieving interoperability among e–government information systems. The EU finances the ESSIF–LAB to expedite the development, integration, and adoption of SSI technologies. In addition, the EC supports the development of the eIDAS bridge that integrates with ESSIF. eIDAS bridges assist with signing the verifiable credentials and support in assessing the trustworthiness of the verifiable credentials. Their arrangement transforms decentralized identifiers into verifiable credentials and ensures the legal validity of electronic documents and cross–border trust services. ESSIF, alongside eIDAS, leads the effort of accomplishing the vision of SSI in the EU and expanding EBSI's capabilities with state of the art digital identity services.

The NIS Directive requires the operators of essential services and digital service providers to strengthen their network and information systems. It also expects that EU member states develop CSIRTs and participate in the NIS Cooperation Group to collaborate with one another. The EC recognizes the significant impact of the NIS Directive on developing cybersecurity capabilities and improving the security posture of organizations across the EU. However, EU member states differentiate their approaches regarding the transposition of the directive into national legislation. The fragmentation of the regulatory landscape leads to inconsistencies in the requirements and incident reporting procedures. In particular, it affects and confuses organizations that provide services across multiple EU member states. Also, the expansion of the threat landscape urges the need for reinforced security measures. Therefore, the EC recommends extending the scope of the existing directive, eliminating the differentiation between the operators of essential services and digital service providers, increasing the requirements for organizations, and establishing a risk–based approach. The arrangement of IAM concepts, principles, mechanisms, and technologies can support organizations to withstand sophisticated attacks and comply with regulatory obligations.

The AIA is the first legal framework that approaches the uncertainties associated with AI. The prediction, optimization, allocation, and personalization capabilities of AI tech–

nologies lead to numerous economic, societal, and environmental benefits. However, there are significant risks concerning health and safety alongside the potential implications on the rights and freedoms of individuals. Moreover, the existing legislation does not address AI technologies precisely. In conjunction with the reasonable technical complexity and the potential lack of transparency that pertain to AI applications, the before–mentioned challenges usually cause legal uncertainty for organizations and obstruct the work of supervisory authorities. The latest regulatory proposal formulates an extensive scope of application, as it concerns providers and users of AI systems located within and outside the EU under specific conditions. The proposal introduces a risk–based approach with four distinct levels of risk classification. Although the regulation might be subject to additional adjustments before its adoption, it reveals the possibility of influencing the identity analytics processes and the AI–powered functionalities of IAM, IGA, and PAM systems during the next few years.

Table 4.1: Policy Developments and Initiatives — Summary

Name	Description	Emerging Approaches
eIDAS Regulation Revision	The revision of eIDAS modernizes the framework for digital identity in Europe. As the expectations around privacy and data protection increase, the EC seizes the opportunity to align eIDAS with disruptive technologies such as blockchain for IdM that can actualize SSI.	Identity and Blockchain
ESSIF Development	ESSIF and the revision of eIDAS help establish the SSI model in the EU and empower EBSI with innovative services regarding digital identity. Blockchain allows for user–centric IdM, meets the expectations of multiple stakeholders, and increasingly contributes to a paradigm shift in IdM and IAM.	Identity and Blockchain

NIS Directive Revision	The frequent cybersecurity challenges and the extensive threat landscape stress the importance of an updated legislative act. The revision of the NIS Directive increases the expectations regarding information security and risk management. The emerging approaches to IAM can help organizations withstand sophisticated attacks and comply with regulatory obligations.	Continuous Authentication, Passwordless Authentication, Attribute-Based Access Control, JIT Access, Zero Trust Model
AI Regulation Proposal	The proposed AIA addresses the challenges concerning AI applications. It introduces a risk-based approach with four distinct classification levels. Although the proposed regulation might receive adjustments before adoption, the legislation is likely to influence identity analytics and the AI-powered capabilities of IAM, IGA, and PAM systems.	Identity Analytics, Identity and Artificial Intelligence

5 Conclusions

5.1 Contributions

This master's thesis concludes with exploring the fundamental IAM aspects, identifying the emerging approaches to IAM, and examining the direction of the EU towards the state of the art IAM concepts, principles, mechanisms, and technologies.

The thesis connected the traditional approaches to IAM for e–government services. It compared the definitions of digital identity—as perceived by different institutions for technical standards—and explained the relationships among identities, identifiers, credentials, and attributes. Upon discussing the roles of the IdP and the SP (also known as the RP), the thesis covered the centralized, federated, and decentralized approaches to IdM. It featured the authoritative sources that act as the source of truth regarding identities, explained the primary responsibilities that fall under the scope of ILM and include creating, facilitating, updating, and revoking identities, and explained the meaning of JML who enter an organization, transfer within an organization or across organizations, or leave an organization. The thesis also looked into authentication matters, as it described the distinct factors of authentication and the importance of SFA, MFA, step–up authentication, and adaptive authentication. As far as authorization is concerned, the thesis mentioned PoLP that dictates the assignment of the minimum amount of permissions, SoD that requires more than one person for performing high–risk activities, and the well–established MAC, DAC, and RBAC models that help regulate access to resources. Regarding federation, the thesis considered FIM for the cooperation among IdPs and SPs and explained the main differences from SSO.

Moreover, the thesis reflected the emerging approaches to IAM for e–government services. It introduced the potential contributions of blockchain to IAM and discussed the decentralization of IdM that empowers people with enhanced control over their identities. The thesis covered continuous authentication that works alongside the more conventional step–up and adaptive authentication processes and leverages analytics, AI–powered technologies, and multimodal biometrics for the non–stop validation of identities. In addition, it explored passwordless authentication that strives to eliminate the traditional weaknesses associated with password–based authentication while improving the broader experience for users. The thesis mentioned ABAC that establishes fine–grained control, offers compatibility with separate access control models,

and uses predefined policy statements that, in turn, correlate multiple subject attributes, resource attributes, and environmental attributes to approve or deny access. Besides, the thesis explored JIT access that orchestrates the assignment and the subsequent removal of elevated privileges, contributes to the maintenance of ZSP, supports the enforcement of PoLP, and inspires the establishment of ZTM. It also explored ZTM that symbolizes the paradigm shift to perimeterless security, necessitates the adoption of tight measures regarding IAM, enforces PoLP to the greatest extent, protects resources continuously, and prevents the execution of several kinds of attacks. The thesis recognized the importance of analytics in the context of IAM and IGA since it supports organizations with their compliance efforts, allows them to obtain an increased understanding of identities, and guides them towards detecting potential weaknesses such as inappropriate access rights, excess privileges, and SoD conflicts. Finally, it discussed the contributions of AI technologies to IAM and IGA that take the role of analytics further, generate automated recommendations to decrease the manual work required by administrators and reviewers, and compare identities against behavioural patterns to detect any fraudulent activity.

Furthermore, the thesis examined some of the latest EU policies and initiatives and connected them to the emerging approaches to IAM. It introduced the revision of the eIDAS Regulation, explained its potential benefits, elaborated on the significance of modernizing the framework, and made an association with the emergence of blockchain for IdM. Then, the thesis mentioned the development of ESSIF that expedites the actualization of SSI in the EU and contributes to the diversification of EBSI's services around digital identity. It also reflected the relationship between eIDAS and ESSIF. Following ESSIF, the thesis discussed the revision of the NIS Directive that intends to strengthen the requirements regarding information security and risk management, expand the scope of application to include additional categories of organizations, harmonize the legislative implementation across the EU, and foster cooperation among member states. Also, the thesis explored the AIA that encounters the challenges of AI, encourages the development and deployment of transparent AI applications, and protects the fundamental rights of individuals. It concluded with an assumption that the proposed legal framework on AI is likely to influence identity analytics and the AI-powered capabilities of IAM, IGA, and PAM systems.

5.2 Recommendations

The introductory chapter mentioned that the particular characteristics of this master's thesis imposed restrictions on identifying and describing the concepts, principles, mechanisms, and technologies that relate to IAM and e-government services. In essence,

the author could not prepare an exhaustive catalogue of the established and emerging approaches to IAM. Instead, he selected and presented—what he assumed to be—the most significant elements of the comprehensive IAM domain. Regardless, the second and the third chapter of this master's thesis managed to provide an up–to–date overview of the IAM domain and share adequate information on the ongoing research and development priorities. Regarding future studies, the author recommends extending the information that pertains to IAM and e–government services. As the author sometimes could not obtain access to specific research papers, he especially suggests considering additional academic databases and libraries to the extent possible. The further incorporation of research papers and studies may complement the material from reputable IAM, IGA, and PAM vendors that the thesis emphasized.

As far as the multiple e–government services in the EU are concerned, this master's thesis did not perform any case study review and, therefore, could not observe any direct connections to the state of the art IAM concepts, principles, mechanisms, and technologies. Regrettably, at the time of writing, there was not enough documentation publicly available that elaborated on the exact IAM specifications (e.g., architecture, requirements, and technologies) of the different e–government services across the EU. Further studies have the opportunity to perform the necessary observations and present their findings accordingly. For this purpose, researchers might need to collect and analyze the appropriate documentation from the participating organizations. In addition, researchers may arrange interviews with the corresponding system experts to obtain an increased understanding of the IAM inner workings. The fulfilment of the before–mentioned recommendations might require the obtainment of security clearances in advance and, therefore, it cannot be guaranteed that researchers receive appropriate access. Although not associated with the initial purposes of this master's thesis, researchers might also consider reaching out to the different categories of stakeholders of e–government services—including public sector employees and citizens—to acknowledge their perspectives and determine whether the respective information systems can benefit from further adjustments.

Concerning the direction that the EU sets towards embracing the state–of–the–art IAM concepts, principles, mechanisms, and technologies, this master's thesis covered the development of three relevant policies and one technical framework. In particular, the eIDAS Regulation and the NIS Directive already exist and are expected to undergo revision. In addition, there is a proposal for the establishment of AIA as the first regulatory framework. Besides, as of this writing, the first version of ESSIF appears to be limited in terms of functionality. Consequently, the author concentrated on providing a high–level overview of the before–mentioned policy developments alongside the current specification of ESSIF. He recommends expanding the range of the review and looking into additional policy developments and initiatives. Moreover, researchers

may concentrate on the eIDAS Regulation and the NIS Directive and consider further aspects relating to IAM. As soon as the proposals for the revision of the eIDAS Regulation and the NIS Directive—as well as the ones for AIA and ESSIF—progress and pass the adoption stage, future studies might seize the opportunity to present meaningful insights into their implementation and enforcement.

Bibliography

[1] M. Laurent and S. Bouzefrane, "Digital Identity," in *Digital Identity Management*. Elsevier, 2015, pp. 11–36.

[2] N. N. G. de Andrade, "Legal Aspects," in *Electronic Identity*. Springer London, 2014, pp. 4–5.

[3] Gartner. (2021). "Identity and Access Management (IAM)," [Online]. Available: https://www.gartner.com/en/information-technology/glossary/identity-and-access-management-iam (visited on 06/25/2021).

[4] B. Priem, R. Leenes, E. Kosta, and A. Kuczerawy, "The Identity Landscape," in *Digital Privacy: PRIME – Privacy and Identity Management for Europe*, J. Camenisch, R. Leenes, and D. Sommer, Eds. Springer Berlin Heidelberg, 2011, pp. 33–51.

[5] Okta. (2020). "User Identity and Access Management: A Bridge to Government IT Modernization," [Online]. Available: https://www.okta.com/resources/whitepaper/user-identity-and-access-management-government-it-modernization (visited on 06/25/2021).

[6] B. Zwattendorfer, K. Stranacher, and A. Tauber, "Towards a Federated Identity as a Service Model," in *Technology-Enabled Innovation for Democracy, Government and Governance*, A. Kő, C. Leitner, H. Leitold, and A. Prosser, Eds., Springer Berlin Heidelberg, 2013, pp. 45–55.

[7] S. Papagiannidis, J. Harris, and D. Morton, "WHO Led the Digital Transformation of your Company? A Reflection of IT Related Challenges during the Pandemic," *International Journal of Information Management*, vol. 55, pp. 2–4, 2020.

[8] L. Goasduff. (2021). "Key Priorities for IAM Leaders in 2021," [Online]. Available: https://www.gartner.com/smarterwithgartner/key-priorities-for-iam-leaders-in-2021/ (visited on 06/25/2021).

[9] International Telecommunication Union. (2010). "Recommendation X.1252 - Baseline Identity Management Terms and Definitions," [Online]. Available: https://www.itu.int/rec/T-REC-X.1252-201004-I (visited on 06/25/2021).

[10] National Institute of Standards and Technology. (2017). "NIST Special Publication 800–63–3 - Digital Identity Guidelines," [Online]. Available: https://doi.org/10.6028/NIST.SP.800–63–3 (visited on 06/25/2021).

[11] International Organization for Standardization. (2019). "ISO/IEC 24760–1:2019 — A Framework for Identity Management — Part 1: Terminology and Concepts," [Online]. Available: https://www.iso.org/standard/77582.html (visited on 06/25/2021).

[12] E. Bertino and K. Takahashi, "What Is Identity Management?" In *Identity Management: Concepts, Technologies, and Systems*. Artech House Publishers, 2011, p. 24.

[13] Diego Poza. (2018). "The Difference Between Web Access Management and Identity Management," [Online]. Available: https://auth0.com/blog/the–difference–between–wam–and–idm (visited on 06/25/2021).

[14] P. Armstead. (2020). "What Is Identity Governance and Administration?" [Online]. Available: https://www.okta.com/blog/2020/10/identity–governance–and–administration/ (visited on 06/25/2021).

[15] M. J. Haber, "Privileged Attack Vectors," in *Privileged Attack Vectors: Building Effective Cyber–Defense Strategies to Protect Organizations*, 2nd ed. Apress, 2020, pp. 7–10.

[16] E. Bertino and K. Takahashi, "Stakeholders and Their Requirements," in *Identity Management: Concepts, Technologies, and Systems*. Artech House Publishers, 2011, p. 27.

[17] P. Siriwardena, "Designing Security for APIs," in *Advanced API Security: OAuth 2.0 And Beyond*. Apress, 2020, p. 59.

[18] D. Pöhn and W. Hommel, "An Overview of Limitations and Approaches in Identity Management," in *Proceedings of the 15th International Conference on Availability, Reliability and Security*, Association for Computing Machinery, 2020, pp. 3–6.

[19] E. Osmanoglu, "IAM Framework, Key Principles, and Definitions," in *Identity and Access Management: Business Performance Through Connected Intelligence*. Syngress, 2013, pp. 52–53.

[20] J. Jensen, "Identity Management Lifecycle – Exemplifying the Need for Holistic Identity Assurance Frameworks," in *Information and Communication Technology*, K. Mustofa, E. J. Neuhold, A. M. Tjoa, E. Weippl, and I. You, Eds., Springer Berlin Heidelberg, 2013, pp. 344–347.

[21] M. J. Haber and D. Rolls, "Provisioning and Fulfillment," in *Identity Attack Vectors: Implementing An Effective Identity And Access Management Solution*. Apress, 2020, pp. 67–68.

[22] M. Schwartz, "Components of an Identity Service," in *Securing the Perimeter: Deploying Identity and Access Management with Free Open Source Software*. Apress, 2019, pp. 2–8.

[23] S. Boonkrong, "Methods and Threats of Authentication," in *Authentication and Access Control: Practical Cryptography Methods and Tools*. Apress, 2021, pp. 45–52.

[24] I. V. Sandoval, B. Stojkovski, and G. Lenzini, "A Protocol to Strengthen Password–Based Authentication," in *Emerging Technologies for Authorization and Authentication*, A. Saracino and P. Mori, Eds. Springer International Publishing, 2018, pp. 38–40.

[25] D. Dasgupta, A. Roy, and A. Nag, "Biometric Authentication," in *Advances in User Authentication*. Springer International Publishing, 2017, pp. 38–69.

[26] D. Dasgupta, A. Roy, and A. Nag, "Multi–Factor Authentication," in *Advances in User Authentication*. Springer International Publishing, 2017, pp. 186–188.

[27] National Institute of Standards and Technology. (2019). "Multifactor Authentication for E–Commerce - Risk–Based, FIDO Universal Second Factor Implementations for Purchasers," [Online]. Available: https://doi.org/10.6028/NIST.SP.1800–17 (visited on 06/25/2021).

[28] A. Akers. (2020). "What Is Step–Up Authentication, and When Should You Use It?" [Online]. Available: https://auth0.com/blog/what–is–step–up–authentication–when–to–use–it (visited on 06/25/2021).

[29] Andy Zindel. (2017). "What is Adaptive Authentication?" [Online]. Available: https://www.centrify.com/blog/what–is–adaptive–authentication (visited on 06/25/2021).

[30] M. Miller. (2021). "What Is Least Privilege & Why Do You Need It?" [Online]. Available: https://www.beyondtrust.com/blog/entry/what–is–least–privilege (visited on 06/25/2021).

[31] S. Ferroni. (2016). "Implementing Segregation of Duties: A Practical Experience Based on Best Practices," [Online]. Available: https://www.isaca.org/resources/isaca–journal/issues/2016/volume–3/implementing–segregation–of–duties–a–practical–experience–based–on–best–practices (visited on 06/25/2021).

[32] National Institute of Standards and Technology. (2020). "NIST Special Publication 800–53 Rev. 5 – Security and Privacy Controls for Information Systems and Organizations," [Online]. Available: https://doi.org/10.6028/NIST.SP.800–53r5 (visited on 06/25/2021).

[33] Okta. (2021). "What Is Role–Based Access Control (RBAC)?" [Online]. Available: https://www.okta.com/identity–101/what–is–role–based–access–control–rbac (visited on 06/25/2021).

[34] A. A. Malik, H. Anwar, and M. A. Shibli, "Federated Identity Management (FIM): Challenges and Opportunities," in *2015 Conference on Information Assurance and Cyber Security (CIACS)*, IEEE, 2015, pp. 75–76.

[35] Oracle. (2018). "What is Security Assertion Markup Language (SAML)?" [Online]. Available: https://www.oracle.com/security/cloud–security/what–is–saml (visited on 06/25/2021).

[36] M. Spasovski, "Benefits of OAuth 2.0," in *OAuth 2.0 Identity and Access Management Patterns*. Packt Publishing, 2013, pp. 9–11.

[37] Y. Wilson and A. Hingnikar, "SAML 2.0," in *Solving Identity Management In Modern Applications: Demystifying OAuth 2.0, OpenID Connect, And SAML 2.0*. Apress, 2019, pp. 105–110.

[38] A. Buecker, P. Ashley, and N. Readshaw. (2008). "Federated Identity and Trust Management," [Online]. Available: https://www.redbooks.ibm.com/abstracts/redp3678.html (visited on 06/25/2021).

[39] E. McKeown. (2021). "Single Sign–on vs. Federated Identity Management: The Complete Guide," [Online]. Available: https://www.pingidentity.com/en/company/blog/posts/2021/sso–vs–federated–identity–management (visited on 06/25/2021).

[40] R. Neisse, G. Steri, and I. Nai–Fovino, "Blockchain–based Identity Management and Data Usage Control," in *Privacy and Identity Management: The Smart Revolution*, M. Hansen, E. Kosta, I. Nai–Fovino, and S. Fischer–Hübner, Eds. Springer International Publishing, 2017, pp. 237–238.

[41] W. L. Sim, H. N. Chua, and M. Tahir, "Blockchain for Identity Management: The Implications to Personal Data Protection," in *2019 IEEE Conference on Application, Information and Network Security (AINS)*, IEEE, 2019, pp. 30–35.

[42] M. Kuperberg, "Blockchain–Based Identity Management: A Survey From the Enterprise and Ecosystem Perspective," *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 1024–1027, 2020.

[43] S. E. Haddouti and M. D. E.–C. E. Kettani, "Analysis of Identity Management Systems Using Blockchain Technology," in *2019 International Conference on Advanced Communication Technologies and Networking (CommNet)*, IEEE, 2019, pp. 2–6.

[44] Y. Liu, D. He, M. S. Obaidat, N. Kumar, M. K. Khan, and K.–K. Raymond Choo, "Blockchain–Based Identity Management Systems: A Review," *Journal of Network and Computer Applications*, vol. 166, pp. 6–9, 2020.

[45] M. Nuss, A. Puchta, and M. Kunz, "Towards Blockchain–Based Identity and Access Management for Internet of Things in Enterprises," in *Trust, Privacy and Security in Digital Business*, S. Furnell, H. Mouratidis, and G. Pernul, Eds., Springer International Publishing, 2018, pp. 176–180.

[46] R. Pakkath. (2019). "Self–Sovereign Identity: A Distant Dream or an Immediate Possibility?" [Online]. Available: https://www.idaptive.com/blog/self–sovereign–identity–distant–dream–immediate–possibility (visited on 06/25/2021).

[47] Castle. (2020). "A Guide to Continuous Identity Protection For Your Online Business," [Online]. Available: https://castle.io/resources/a–guide–to–continuous–identity–protection–for–your–online–business (visited on 06/25/2021).

[48] N. Fisher. (2018). "What is Continuous Authentication?" [Online]. Available: https://www.okta.com/blog/2018/03/what–is–continuous–authentication (visited on 06/25/2021).

[49] G. Dahia, L. Jesus, and M. P. Segundo, "Continuous Authentication using Biometrics: An Advanced Review," *WIREs Data Mining and Knowledge Discovery*, vol. 10, no. 4, pp. 4–18, 2020.

[50] R. Ryu, S. Yeom, S.–H. Kim, and D. Herbert, "Continuous Multimodal Biometric Authentication Schemes: A Systematic Review," *IEEE Access*, vol. 9, pp. 10–13, 2021.

[51] K. McGuinness. (2020). "The Path to Continuous Authentication: Solving the Best of Breed Problem," [Online]. Available: https://www.okta.com/blog/2020/06/the–path–to–continuous–authentication–solving–the–best–of–breed–problem (visited on 06/25/2021).

[52] R. Smith. (2020). "The Future of Zero Trust: Continuous Authentication," [Online]. Available: https://www.signalsciences.com/blog/future–of–zero–trust–continuous–authentication (visited on 06/25/2021).

[53] M. Campbell, "Putting the Passe Into Passwords: How Passwordless Technologies Are Reshaping Digital Identity," *Computer*, vol. 53, no. 8, pp. 90–92, 2020.

[54] S. G. Lyastani, M. Schilling, M. Neumayr, M. Backes, and S. Bugiel, "Is FIDO2 the Kingslayer of User Authentication? A Comparative Usability Study of FIDO2 Passwordless Authentication," in *2020 IEEE Symposium on Security and Privacy (SP)*, IEEE, 2020, pp. 278–280.

[55] S. Sham. (2020). "Magic Links: Passwordless Login for Your Users," [Online]. Available: https://www.okta.com/blog/2020/09/magic-links (visited on 06/25/2021).

[56] Auth0. (2020). "Passwordless Authentication with Magic Links," [Online]. Available: https://auth0.com/docs/connections/passwordless/guides/email-magic-link (visited on 06/25/2021).

[57] National Institute of Standards and Technology. (2014). "NIST Special Publication 800-162 - Guide to Attribute Based Access Control (ABAC) Definition and Considerations," [Online]. Available: https://doi.org/10.6028/NIST.SP.800-162 (visited on 06/25/2021).

[58] K. Casey. (2020). "What Is Attribute-Based Access Control (ABAC)?" [Online]. Available: https://www.okta.com/blog/2020/09/attribute-based-access-control-abac (visited on 06/25/2021).

[59] Axiomatics. (2016). "The Benefits of Fine-Grained Dynamic Authorization: An Introduction to Attribute Based Access Control," [Online]. Available: https://www.axiomatics.com/blog/the-benefits-of-fine-grained-dynamic-authorization-an-introduction-to-attribute-based-access-control (visited on 06/25/2021).

[60] D. Servos and S. L. Osborn, "Current Research and Open Problems in Attribute-Based Access Control," *ACM Computing Surveys*, vol. 49, no. 4, pp. 26–32, 2017.

[61] SailPoint. (2021). "What is Attribute-Based Access Control?" [Online]. Available: https://www.sailpoint.com/identity-library/what-is-attribute-based-access-control (visited on 06/25/2021).

[62] Q. N. T. Thi and T. K. Dang, "Towards a Fine-Grained Privacy-Enabled Attribute-Based Access Control Mechanism," in *Transactions on Large-Scale Data- and Knowledge-Centered Systems XXXVI: Special Issue on Data and Security Engineering*, A. Hameurlain, J. Küng, R. Wagner, T. K. Dang, and N. Thoai, Eds. Springer Berlin Heidelberg, 2017, pp. 52–72.

[63] M. Gupta, F. M. Awaysheh, J. Benson, M. Alazab, F. Patwa, and R. Sandhu, "An Attribute-Based Access Control for Cloud Enabled Industrial Smart Vehicles," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 6, pp. 1–4, 2021.

[64] Y. Wang, Q. Sun, Y. Ma, J. Zhang, Z. Liu, and J. Xue, "Security Enhanced Cloud Storage Access Control System Based on Attribute Based Encryption," in *2018 International Conference on Big Data and Artificial Intelligence (BDAI)*, IEEE, 2018, pp. 52–57.

[65] M. Miller. (2019). "Just–In–Time Privileged Access Management (JIT PAM): The Missing Piece to Achieving "True" Least Privilege & Maximum Risk Reduction," [Online]. Available: https://www.beyondtrust.com/blog/entry/just-in-time-privileged-access-management-jit-pam-the-missing-piece-to-achieving-true-least-privilege-maximum-risk-reduction (visited on 06/25/2021).

[66] BeyondTrust. (2020). "The Guide to Just–In–Time Privileged Access Management," [Online]. Available: https://www.beyondtrust.com/resources/whitepapers/guide-to-just-in-time-privileged-access-management (visited on 06/25/2021).

[67] C. Owen. (2020). "Just–in–Time (JIT) Access: Zero Standing Privileges," [Online]. Available: https://www.centrify.com/blog/just-time-jit-zero-standing-privileges (visited on 06/25/2021).

[68] Dan Ritch. (2020). "Just–in–Time Privileged Access Eliminates the Danger of Standing Privileges," [Online]. Available: https://thycotic.com/company/blog/2020/06/23/jit-just-in-time-and-privileged-access (visited on 06/25/2021).

[69] M. Kaufmann. (2020). "Time–Limited Privileged Access Management: The Path To Zero Trust," [Online]. Available: https://saviynt.com/time-limited-privileged-access-management-the-path-to-zero-trust (visited on 06/25/2021).

[70] National Institute of Standards and Technology. (2020). "NIST Special Publication 800–207 - Zero Trust Architecture," [Online]. Available: https://doi.org/10.6028/NIST.SP.800-207 (visited on 06/25/2021).

[71] Ping Identity. (2021). "Security Leader's Guide to the Zero Trust Model," [Online]. Available: https://www.pingidentity.com/en/resources/client-library/guides/3243-security-leaders-guide-to-IAM.html (visited on 06/25/2021).

[72] Okta. (2021). "Getting Started with Zero Trust: Never Trust, Always Verify," [Online]. Available: https://www.okta.com/resources/whitepaper/zero-trust-with-okta-modern-approach-to-secure-access (visited on 06/25/2021).

[73] S. Mehraj and M. T. Banday, "Establishing a Zero Trust Strategy in Cloud Computing Environment," in *2020 International Conference on Computer Communication and Informatics (ICCCI)*, IEEE, 2020, pp. 3–5.

[74] S. Flaster. (2020). "A Zero Trust Approach to Protecting Cloud Identities Begins with Least Privilege," [Online]. Available: https://www.cyberark.com/resources/blog/a-zero-trust-approach-to-protecting-cloud-identities-begins-with-least-privilege (visited on 06/25/2021).

[75] I. Ahmed, T. Nahar, S. S. Urmi, and K. A. Taher, "Protection of Sensitive Data in Zero Trust Model," in *2020 International Conference on Computing Advancements (ICCA)*, Association for Computing Machinery, 2020, pp. 3–4.

[76] F. Briguglio. (2019). "Balancing Zero Trust with a Strong Identity Strategy and AI," [Online]. Available: https://www.sailpoint.com/blog/zero-trust-identity-governance (visited on 06/25/2021).

[77] Erika Weiler and Priti Patil. (2019). "Uncover Access Risks Across your Security Environment with Identity Analytics," [Online]. Available: https://community.ibm.com/community/user/security/blogs/erika-weiler1/2019/07/25/cloudidentityanalyze (visited on 06/25/2021).

[78] D. Lee. (2016). "Identity and Analytics: Looking to the Future of IAM," [Online]. Available: https://www.sailpoint.com/blog/identity-analytics (visited on 06/25/2021).

[79] Erika Weiler. (2020). "Prioritize Identity Analytics for Greater IGA Return on Investment," [Online]. Available: https://community.ibm.com/community/user/security/blogs/erika-weiler1/2020/07/24/prioritize-identity-analytics-for-greater-roi (visited on 06/25/2021).

[80] SailPoint. (2020). "Intelligent AI-Driven Identity Governance," [Online]. Available: https://www.sailpoint.com/identity-library/intelligent-ai-driven-identity-governance (visited on 06/25/2021).

[81] Yash Prakash. (2021). "The Future Is Now: Powering Smart Identity With Analytics, AI, and ML," [Online]. Available: https://saviynt.com/the-future-is-now-powering-smart-identity-with-analytics-ai-and-ml (visited on 06/25/2021).

[82] ForgeRock. (2020). "Artificial Intelligence-Driven Security and Compliance," [Online]. Available: https://www.forgerock.com/solutions/identity-governance-administration-iga (visited on 06/25/2021).

[83] Idaptive. (2019). "The Rise of AI-Powered Identity Security," [Online]. Available: https://www.cyberark.com/resources/white-papers/the-rise-of-ai-powered-identity-security (visited on 06/25/2021).

[84] OneLogin. (2021). "Next Generation Identity and Access Management: The Trusted Experience Platform," [Online]. Available: https://www.onelogin.com/resource-center/ebooks/trusted-experience (visited on 06/25/2021).

[85] Publications Office of the European Union. (2018). "European Union Directives," [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=legissum:l14527 (visited on 06/25/2021).

[86] Publications Office of the European Union. (2015). "European Union Regulations," [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l14522 (visited on 06/25/2021).

[87] J. Carretero, G. Izquierdo-Moreno, M. Vasile-Cabezas, and J. G. Blas, "Federated Identity Architecture of the European eID System," *IEEE Access*, vol. 6, pp. 16-17, 2018.

[88] European Commission. (2021). "Trust Services and Electronic Identification," [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/trust-services-and-eid (visited on 06/25/2021).

[89] European Commission. (2020). "Digital Identity and Trust: Commission Launches Public Consultation on the eIDAS Regulation," [Online]. Available: https://digital-strategy.ec.europa.eu/en/news/digital-identity-and-trust-commission-launches-public-consultation-eidas-regulation (visited on 06/25/2021).

[90] European Commission. (2020). "EU Digital ID Scheme for Online Transactions across Europe," [Online]. Available: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12528 (visited on 06/25/2021).

[91] ENISA. (2020). "eIDAS Compliant eID Solutions," [Online]. Available: https://www.enisa.europa.eu/publications/eidas-compliant-eid-solutions (visited on 06/25/2021).

[92] European Commission. (2020). "European Self-Sovereign Identity Framework (ESSIF) - Technical Specification (1)," [Online]. Available: https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=262505735 (visited on 06/25/2021).

[93] European Commission. (2020). "ESSIF Orientation Vision Text," [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/ESSIF+Orientation+Vision+Text (visited on 06/25/2021).

[94] European Commission. (2020). "European Self Sovereign Identity Framework Laboratory," [Online]. Available: https://cordis.europa.eu/project/id/871932 (visited on 06/25/2021).

[95] European Commission. (2020). "European Self-Sovereign Identity Framework (ESSIF) - Technical Specification (15)," [Online]. Available: https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=262505862 (visited on 06/25/2021).

[96] European Commission. (2021). "About SSI eIDAS Bridge," [Online]. Available: https://joinup.ec.europa.eu/collection/ssi-eidas-bridge/about (visited on 06/25/2021).

[97] European Commission. (2021). "NIS Directive," [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/nis-directive (visited on 06/25/2021).

[98] European Commission. (2020). "Cybersecurity - Review of EU Rules on the Security of Network and Information Systems," [Online]. Available: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12475-Cybersecurity-review-of-EU-rules-on-the-security-of-network-and-information-systems_en (visited on 06/25/2021).

[99] European Commission. (2020). "Proposal for Directive on Measures for High Common Level of Cybersecurity across the Union," [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union (visited on 06/25/2021).

[100] European Commission. (2021). "Revised Directive on Security of Network and Information Systems (NIS2)," [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/revised-directive-security-network-and-information-systems-nis2 (visited on 06/25/2021).

[101] ENISA. (2020). "NIS Investments," [Online]. Available: https://www.enisa.europa.eu/publications/nis-investments/ (visited on 06/25/2021).

[102] European Commission. (2021). "Europe Fit for the Digital Age: Commission Proposes New Rules and Actions for Excellence and Trust in Artificial Intelligence," [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1682 (visited on 06/25/2021).

[103] European Commission. (2020). "Artificial Intelligence - Ethical and Legal Requirements,"[Online]. Available: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements_en (visited on 06/25/2021).

[104] European Commission. (2021). "Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence," [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence (visited on 06/25/2021).