2020-08

An Interoperable Identity Management Framework (In the Case of Ethiopian e-governmer

Tsehaye, Asress Tedla

Wisdom at the source of the Blue Nile

BAHIR DAR UNIVERSITY

BAHIR DAR INSTITUTE OF TECHNOLOGY

SCHOOL OF RESEARCH AND POSTGRADUATE STUDIES

Faculty of Computing

An Interoperable Identity Management Framework (In the Case of Ethiopian e-government)

MSc. Thesis

By

Tsehaye Asress Tedla

A Thesis Submitted as a Partial Fulfillment to the Requirements for the Award of the Degree of Master of Science in Information Technology.

Main Advisor: Mekuanint Agegnehu (Ph.D.)

August 2020

Bahir Dar, Ethiopia

BAHIR DAR UNIVERSITY
BAHIR DAR INSTITUTE OF TECHNOLOGY
SCHOOL OF GRADUATE STUDIES
FACULTY OF COMPUTING

Approval of thesis for defense result

I hereby confirm that the changes required by the examiners have been carried out and incorporated in the final thesis.

Name of Student Tsehaye Asress Tedla Signature________ Date 14/11/2023As members of the board of examiners, we examined this thesis entitled "**An Interoperable Identity Management Framework (In the Case of Ethiopian e-government)**" by Tsehaye Asress Tedla. We hereby certify that the thesis is accepted for fulfilling the requirements for the award of the degree of Master of Science in "Information Technology".

Board of Examiners

Name of Advisor	Signature	Date
Mekuanint Agegnehu (PhD)		05/03/2016
Name of External examiner	Signature	Date
Elefelious Getachew (PhD)		05/03/2016
Name of Internal Examiner	Signature	Date
Mekonnen Wagaw (PhD)		14/11/2023
Name of Chairperson	Signature	Date
Gebeyehu Belay (PhD)		14/11/2023
Name of Chair Holder	Signature	Date
Abdulkerim.M		14/11/2023
Name of Faculty Dean	Signature	Date
[illegible] K.		14/11/2023

Faculty Stamp

Bahir Dar University
Technology

Acknowledgments

I would like first to express my profound sense of gratitude towards my advisor Mekuanint Agegnehu (Ph.D) for his direction, kindness, and encouragement throughout the time this research work was carried out.

I would also like to thank all my family, friends, and colleagues for their commitment and contribution to the success of the graduate program.

Abstract

Identity management and integrated technologies are the basic building blocks in the field of e-Government, as they constitute secure and reliable access to online services. The implementation of integrated identity management is complex due to the involvement of multiple organizations with heterogeneous technologies, different data sources and interoperable records, sensitive user data, legal and regulatory issues, and numerous security issues. Though multiple private and governmental identity management (IDM) frameworks and technologies developed and implemented for backend organizational integration and service delivery, integrating ministries and agencies effectively and sustainably is still researchable. In this thesis, an interoperable identity management (IDM) framework is proposed by incorporating all the requirements from the administrative, technical, and security perspectives. The proposed framework can integrate the fragmented government systems between or/ and among ministries and agencies for better public service delivery in the context of electronic government. This thesis follows the design science approach. The designed framework was demonstrated and evaluated by technical experts using design science framework evaluation parameters such us completeness, usability, and interoperability.

Table of Contents

List of Figures

Abbreviations

DoS	Denial of Service
EGDI	Electronic Government Development Index
E-Government	Electronic Government
EIdM	Electronic Identity Management
E-Service	Electronic Service
G2B	Government to Business
G2C	Government to Citizen
G2G	Government to Government
IDM	Identity Management
IDP	Identity Provider
IAM	Identity and Access Management
IS	Information system
MCIT	Ministry of Information and Communication Technology
RP	Relying Party
SP	Service Provider
SSL	Secure Socket Layer
SAML	Security Assertion Markup Language
TLS	Transport Layer Security
UN	United Nation
XSS	Cross-Site Scripting Language
IEEE	Institute of electrical and electronics engineering
ACM	Association for computing machinery
JSTOR	Journal storage
SSO	single sign-on
FIM	Federated identity management
OAuth	open authorization
WS-Federation	web service federation
SIGTAS	Standard Integrated Government Tax Administration System

Chapter 1

1.1 Introduction

Electronic Government (E-Governmnet) is all about the use of information technologies and IT applications by the government for the delivery of electronic services and information to the public, businesses, or other government agencies by integrating processes. Besides, it demands safe channels for information exchange without compromising security or exposing sensitive information between government agencies, citizens, and structured organizations. The success of E-Government depends on the citizens' perception of e-Government services, technologies and their interoperability, level of access that citizens and business will have, the overall trust in electronic channels by citizens and business, and their expectations of the types of services that should be delivered and how they should be delivered [1]. In e-government service delivery, identity management technologies determine the access levels of agencies, citizens, and businesses based on rules or agreed authorization requirements [2].

Nowadays, the use of digital identity is imperative for organizations by improving the fragmented and costly identity management solutions which were obstacles in the execution and management of the business process.[3]. Organizations with vertical communication that maintains their own digital identities led to fragmentation and complexities of identity management. Identity management must cut across horizontally distributed organizations to access and share resources among business processes, departments, and even interactions with external partners[3].

Digital identity and identity management systems have defined by multiple international organizations. According to The World Economic Forum (WEF) [4], digital identity defined as a "collection of individual attributes that describe an entity and determine the transactions in which that entity can participate". From a management perspective, identity management system (IDM) can be defined as the enterprise-wide life-cycle management of the digital identity of an entity including its attributes, roles, and associations over a period from creation to the destruction of that identity. Digital Identity Management also provides secure methods to exchange and validate that identity information. Digital identity management requires both technical and legal mechanisms to handle multiple issues related to the identity of an entity [15].

Adopting electronic Identity Management includes the benefits such as storing information in digital form where it can be easily accessed and transferred whenever needed, ensuring a secure, convenient and effective way of identifying an individual, relying party and service provider identities, and safeguarding and protecting access to sensitive information. Besides, it improves the quality of services to be delivered, minimizes management cost, and increases confidence in reliable identification and authorization of users which in turn enables secure and effective day to day information transactions between public agencies. Therefore, by adopting efficient identity management in e-governance, governments can renovate their processes and systems and turn them into a better customer service provider.

The recent development of IT technologies and its expansion within Ethiopia has a significant impact on public service delivery. According to the United Nations e-Government Survey [5], Ethiopia has deemed one of the world's e-government least implemented countries with low E-Government Development Index levels. The advancement of ICTs in the public sector in Ethiopia also presents a significant opportunity for rolling out e-government services. The government of Ethiopia has prioritized three distinct sectors for e-government implementation, government-to-government (G2G), government-to-business (G2B), and government-to-citizen (G2C). Each of these sectors represents a different combination of motivating forces and initiatives. However, some common goals include improving the efficiency, reliability, and quality of services for the respective constituency groups.

Ethiopian government realizes the need to integrate several initiatives to provide a strategic direction for e-Government implementation in the country. It is in this context that the e-Government strategy for Ethiopia has been designed, with a focus on facilitating effective delivery of government services to major customers residents, businesses, and visitors[6].

The strategy envisions the implementation of 219 e-services consisting of seventy-nine (79) informational and one hundred thirty-four (134) transactional services over five years. The implementation is proposed to be done through twelve (12) priority projects and service delivery would be through four channels (Portal, Call center, Mobile devices, and Common service centers) and delivery will be facilitated and strengthened through Six (6) core projects, including National Payment Gateway, Enterprise Architecture framework, Public Key Infrastructure, National Data Set, National Enterprise Service Bus and National integrated Authentication Framework [6].

To achieve government to government (G2G) integration using e-government systems and to enable access and sharing of information requires efficient identity management and access control implementation. Besides, the implementation of a common framework across government agencies and corporations enables smooth delivery of e-government to the public and business sectors.

1.2 Statement of the problem

E-government technologies bring the fragmented government organizations closer together by providing opportunities for the whole of government service delivery and policy integration [5][7].

Based on the study [5][8] government service delivery from various public agencies bundled together as a single, joined-up service in a one-stop-shop creates a simple interaction between people and the government. Achieving such an integrated approach to public service delivery depends on:

- Back-office integration enabled coordinated internal processes using a common organizational and technical platform.
- Interoperable systems.
- An infrastructure that supports the use of electronic identity cards and signatures.

The implementation of effective and sustained service delivery and integration of ministries and agencies remains challenging[5][8].

Identity policy through data and identity protection standards are the base for e-government systems. Additionally, the interaction between ministries and agencies across the e-government information systems is supported by identity management and access control which covers how private data is identified, accessed, shared, and managed based on regulations, policies, trust, collaboration, interoperability, and access management. For instance, in the government of Ethiopia, ministries, and agencies develop, maintain, and archive several fragmented citizens and government data. For example, in most of the region's, customer’s organizational data stores across agencies using fragmented systems, each government organization keeps other details about the same person at the organization. Apart from storing fragmented information, citizens carry different institutional records to get the services of other national or regional public institutions. A single person can have different identities in different organizations.

Designing a governmental interoperable identity management framework with important requirements of administration, technical and security is necessary for integrating and share data of the fragmented governmental systems.

This thesis addresses the following research questions:

- How to design an Identity management framework for Ethiopian e-government for to share and integrate fragmented systems across ministries and agencies?
- How to maintain web security issues in Ethiopia e-government service delivery while sharing and integrating fragmented data across public agencies?

1.3 Objectives of the study

1.3.1 General objective

The main objective of the study is to design an interoperable identity management framework to integrate fragmented systems across ministries and agencies for accessing and sharing of data.

Specific objectives:

- Explore IDM models and integrated technologies that improve collaboration, guarantee interoperability, access, and sharing of data across government ministries and agencies.
- Explore governmental IDM framework main components
- Examine and employ IDM technologies that ensures the major web security threats such as Denial of service (DoS), Cross-Site scripting (XSS), and Man in the middle attack (MIMA) while accessing and sharing of data across ministries and agencies.
- Design and evaluate an interoperable identity management framework

1.4 Scope

This scope of this thesis is designing and implementing an interoperable identity management framework using the design science process. Integration and sharing of data across ministries and agencies horizontally and vertically, accessing and using non-redundant citizen information for public service delivery with the necessary administrative, technical, and security issues in the Ethiopian e-government context are included in the design. However, social and cultural issues, structural interoperability, and biometric authentication which are not covered in this study require further study.

1.5 Significance of the Study

As the government has fragmented identity information in different public institutions and government agencies accessing and sharing this data, interoperability becomes an issue. Integrating and interfacing different government agencies and public institutions where fragmented information is kept is also a fundamental topic to be addressed. Designing a suitable identity management framework based on the necessary administrative, technical, and security requirements.

Chapter 2

2.1 Literature Review

In this study, we used a mixed research approach to gather the requirements from the relying parties and base concepts, issues, protocols related to IDM from the works of literature. An observation has been conducted to gather the existing government organizational integrations and the way citizens are getting services in the selected organizations. Secondly, a detailed literature review conducted to build the basis for the research work by understanding the key concepts, issues, and protocols related to IDM and exploring other important contemporary research work done in the area of IDM. A detailed and rigorous literature review ensured that the current research work was built upon a strong foundation laid by the previous researchers and no important concepts were overlooked.

This chapter describes the literature review process in detail, and the subsequent chapters 3, 4, 5 and 6 describe the essential concepts, important issues, common protocols, and service providers or relying parties perception in particular respectively in the context of this research work with the information derived from the literature review.

2.1.1 Literature Review Process

The literature review was carried out iteratively following the guidelines as suggested in [9] and [10]. A structured and rigorous procedure was followed to do a representative literature review [10] where the most relevant and recent articles containing detailed analyses of the current single sign-on protocols and identity management methods were studied. Only peer-reviewed articles from reputed journals that had a considerable number of citations were selected to ensure the quality of the articles reviewed. Care was taken to select articles that were recent i.e. not older than the year 2010, and all the important keywords and their synonyms were searched in all possible combinations to make certain that no important article was left out. The search for articles continued until no new concepts could be found.

The search for journal articles was done in multiple phases. In the first phase, the top journals and the journal database that would be searched were identified. Suggestion from [9] which lists the top journals and database was considered. The journal database - Elsevier, IEEE, ACM, Google Scholar, and JSTOR were queried as they cover almost all the top journals in the computer science and engineering domain.

In the second phase, a set of initial keywords were identified to query the selected journal database. The keywords were "Single-Sign-On," "SSO," "Federated Identity Management," "FIM," “Identity management,” “Identity and Access Management,”, “IDM,” “‘Eid for e-government” Various combinations of these keywords were used to search the title, author's tags and abstract in the selected databases. From the initial set of selected journal articles, more keywords were selected such as "OpenID Connect," "Security Assertion Markup Language," "SAML," "OpenID," "WS-Federation," “OAuth2” and the search was expanded with new keywords and their combination. These search keywords were also combined with words such as "Organization," "Enterprise," "Review," "Survey," "Analysis," "Compare" to get articles that analyzed multiple protocols and methods. All the searches were done with a filter on the year of publication which was set to the year 2010. The articles found were filtered down by going through their abstract and then further by reading their introduction, results, and conclusion.

In the third phase, the backward reference search [10] was done from the references in the selected articles. The journal articles mentioned in the references were searched based on their title, and their abstracts were reviewed. The articles were selected if they were relevant, had many citations, and appeared to have important theories or information on the foundation of Single Sign-On and Federated Identity Management. Only one level of backward reference search was done.

In the fourth and final phase, forward reference search [9] was done on selected articles to look for the latest information and development in the domain. Articles from the forward search were selected if they were recent and had new concepts and belonged to reputed journals.

All the articles were maintained in an online cloud reference library called "Mendeley" that helped with the management of articles, references, and citations.

2.2 Digital Identity

Identity is a conceptually complex term. It has been defined in different ways and contexts over the years. At a basic level, we can say that identity, in general, is any set of characteristics that define a person and can be used to uniquely identify that person. As a consequence, digital identity would be the digital version of a person's physical identity, the digital representation of the individual[11].

There is a significant number of digital identity definitions: The International Telecommunication Union (ITU) definition emphasizes the context which defines digital identity as a "representation of an entity in the form of one or more attributes that allow the entity or entities to be sufficiently distinguished within the context"[12]. The International Organization for Standardization (ISO) states that digital identity is an "item inside or outside an information and communication technology system, such as a person, an organization, a device, a subsystem, or a group of such items that has a recognizably distinct existence"[4]. This definition implies that, apart from a person, other entities, like devices, might have a digital identity[11]. The World Economic Forum recently defined digital identity as a "collection of individual attributes that describe an entity and determine the transactions in which that entity can participate". This definition, as the previous ones, emphasizes the idea of the usage of the identity. The WEF categorizes attributes into three groups: inherent (age), inherited (behavior), and assigned attributes (ID number). These attributes differ for members of three main user groups: individuals, legal entities, and assets. The attributes enable entities to participate in transactions by proving to their counterparty that they have the specific attributes required for that transaction [11][4].

	For Individual	For legal entities	For assets
Inherent Attribute (Inherent to an entity)	• Age • Height • Date of Birth • Fingerprint	• Industry • Business status	• Nature of the asset • Asset issuer
Accumulated Attributes Attributes developed over time and may change multiple times	• Health records • Preference & behaviors (i.e. telephone metadata)	• Business record • Legal record	• Ownership history • Transaction history
Assigned Attributes • Assigned to the entity but not related to inherent attributes. • Changeable but uniquely identifies the entity at a certain time.	• National Identifier number • Telephone number • Email address	• Identifying numbers • Legal jurisdiction • Directors	• Identifying numbers • Custodianship

Table 1. Digital Identity Attributes [4]

According to [13], digital identity can be categorized into three main categories that can help to isolate specific traits.

- **Foundational digital identity**: is "usually created as part of a national identity scheme or similar, which is based on the formal establishment of identity through the examination of qualifying (breeder) documents such as birth records, marriage certificates, and social security documents";
- **Functional digital identity:** is "created to address the specific needs of an individual sector (for instance, the healthcare or the transportation sectors)";
- **Transactional digital identity**: is "intended to ease the conduct of financial or other transactions (either face to face or across the Internet) across multiple sectors";

2.2.1 Identity Management Systems

In the virtual world, the identity of an entity is the basis for security management and core business functions. Digital identity management, from a technical viewpoint, is defined as a group of technical access control systems and functions to identify an entity accurately with a certain level of assurance and subsequently perform authentication, authorization, or transfer that knowledge to the requesting entity[14]. From a management perspective, it can be defined as the enterprise-wide life-cycle management of the digital identity of an entity including its attributes, roles, and associations over a period from creation to the destruction of that identity. Digital Identity Management also provides secure methods to exchange and validate that identity information. Digital identity management requires both technical and legal mechanisms to handle multiple issues related to the identity of an entity [15]. The [1] defines Identity Management "as the set of rules, procedures, and technical components that implement an organization's policy related to the establishment, use, and exchange of digital identity information."

Digital identity management is one of the most critical aspects of digital security and a major enabler of trusted online business. Successful and efficient digital identity management ensures the security of information resources, user privacy, promotes innovations in online business activities, and improves business interaction by increasing confidence in the exchange of information and execution of business functions. However, digital identity management is complex, and multiple difficult issues must be addressed [15] [16].

Despite the complexities, organizations must get digital identity management right, or else the consequences could be a fragmented and costly identity management solution within the organization that fails to deliver business value and leads to further obstacles in the execution and management of business processes [15].

Invariably, the objective of electronic IdM is to ensure consistent business rules and practices; tightening of control over user-to-applications; automation of business processes to minimize operational costs; enhanced security; improved productivity.

Paul Beynon-Davies [17] have suggested a shift in focus towards analyses of the wider societal implications of IdMS and related social design issues is necessary.

In the past, organizations were divided into vertical silos with each vertical maintain their own digital identities that led to fragmentation and complexities. Nowadays, identity management must cut across horizontally across the organization providing an employee a seamless interaction across different business processes, departments, information resources, and even interaction with external partners [15].

Digital Identity Management essentially consists of three main components [3][18].

- User/Principle/Subject: is the entity that must be identified. An entity could be a human being, an organization, a computing device, software service, or any real or virtual object that can communicate. A user can have one or more identities.
- Identity Provider: They perform the essential function of authenticating a user based on the information that the user presents and subsequently issue authentication assertions for that user. The identity provider is also responsible for maintaining user identities and attributes that are valid and current.
- Service Provider/Relying Party: these are the entities that provide some service to the user by authorizing them based on the authentication information received, attributes of the user, and trust level on the identity provider.

A typical identification process involves a series of exchange of identity information using a standard exchange protocol between the requesting party (service provider) and the asserting party (identity provider) until the requesting party is satisfied with the required level of assurance of the authentication assertions and then makes a decision whether to authorize or deny service to the user [15].

An identifier of an entity uniquely identifies that entity from all other entities present within that domain or system. The scope of an identifier is limited to the system or domain boundary in which it is defined and cannot be meaningfully imported to other domains. Therefore, a user can have multiple identities, each belonging to a different domain and the scope of that identity would depend on the size of the domain. For example, a passport id for a user is unique within the country, an employee id of the same user is unique within the organization, and the user may have other identities such as driving license, email address, and so on [14].

Associated with each identifier is a set of attributes that define the user that is assigned that identity. Attributes are conferred on the user by some different authorities that have the mandate and responsibility to assign one or more of those attributes either by law or industry standards. For example, a university is the right source of the user's education grades and degrees; an employee may assign certain attributes related to job designation, roles, and responsibilities within that organization, the government may assign passport id, the local municipal office may assign date and place of birth and so on. Consequently, a service provider may have to consult multiple sources to validate the different attributes of a user [14][18].

Electronic identity management defined at [19] as "the processes, policies, and technologies used to manage the complete Lifecycle of user identities across a system and to control user access to the system resources by associating their rights and restrictions". In effect, Identity management systems, consisting of the processes and all underlying technologies for the creation, management, and usage of identities and their attributes. Invariably, the objective of electronic IdM is to ensure consistent business rules and practices; tightening of control over user-to-applications; automation of business processes to minimize operational costs; enhanced security; improved productivity.

Researches at [19][18] illustrate the identity formation process and a summary of which is as follows:

- **Enrolment or Registration** - Individuals must go through an initial registration or enrolment process where their biographical footprint, biometric footprint, or a combination of both are captured into the system. The outcome of the enrolment process is the issue of credentials or identifiers to those registered. In effect, enrolment is the process by which an individual is brought within the identity policy and the resulting systems and the eventual issue of credentials and identifiers. The birth of a child or the arrival of a qualified foreign national will usually trigger the enrolment process in a national IDMS [19][18].

- **Authorization** – upon registration, permission, and privileges to access the resources and services are assigned to an individual based on a predefined identification policy[19].
- **Authentication** – This is the process of establishing with a certain degree of confidence in the user's identity or a process that results in a person being accepted as authorized to engage in or perform some activity. Authentication can be done using one or more of the following factors :[18][20]
  a. **Something you know** -the most convenient, easy, and widely used method of authentication where a user to prove its identity must own a secret (password or pin) which is only known to the authentication service. Once the user provides the correct secret associated with its identity, the user is authenticated successfully. This type of authentication is susceptible to replay attack, identity theft, and can be made more secure through a one-time password and challenge-response sequence between the user and the authentication service.
  b. **Something you have** -this authentication method is also known as token-based authentication where the user must own a token/smart card. The user authentication secret is encoded in the token, and the user presents the token to the authentication service to read the secret information and then compare it with the associated identity. On successful validation, the user is authenticated.
  c. **Something you are** -this method of authentication is based on biometric features of an individual such as fingerprint, iris pattern, or voice pattern i.e. things that are unique to an individual. This method is considered to be the most secure, but it applies to human beings only.
- **Access Control** – Authentication process results in the access control process in which a check is made by the system to see if an individual has a valid authorization to access the resource [19][18];

- **Revocation** – on the expiry of individuals' rights or when a person is no more associated with the system, a revocation process is triggered resulting in the credentials and associated rights being rescinded. Such circumstances include the death of a citizen, completion of school, or traveling outside a country for more than a specified period [19][18].

2.3 Approaches to Identity Management

Various forms of governmental and private digital identity management systems have been implemented using various technical and architectural models. This section discusses some of the popular identity management models namely silos, centralized, federated, and user-centric identity management models.

2.3.1 Silo Identity Systems

This is the most common type of Identity Management system designed and functions independently without connecting with other identity systems.[1] Usually implemented in a single firm where identity and services are provided and managed by the service provider alone. The organization plays the role of a service provider and Identity Provider by issuing IDs and managing information on its domain [19].

Siloes systems are simple to deploy from the service provider perspective but inefficient since it creates "identity overload and password fatigue" and identity data has to be maintained in multiple accounts within the organization [1]. Furthermore, as there is no link with other domain identity theft and corruption are extremely limited hence if the domain encounters any security or system failure the consequence is severe [19].

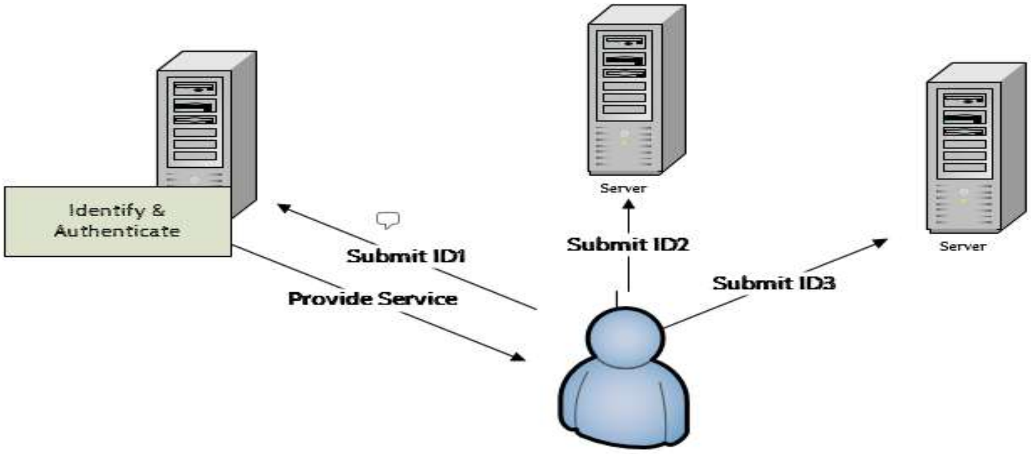


Figure 1. Silo Identity Management Model [20]

2.3.2 Centralized Identity System

The centralized IdMS model is an early attempt to rectify the inherent limitations of silo systems by centralizing the independent databases into a single system. Thus in the centralized model, user data are kept independent of the various application silos, and data are made available to service providers from the central database[19]. Due to the centralized nature of the systems, each user can use the same credentials and identifiers to access different services, whilst all the providers authenticate the client through the same certificate before granting access to their services. Centralized IdMS have evolved with time, given the increasing need to share and reuse identity information. Centralized IdMS is a very common model for storing and managing digital identities [21][14].

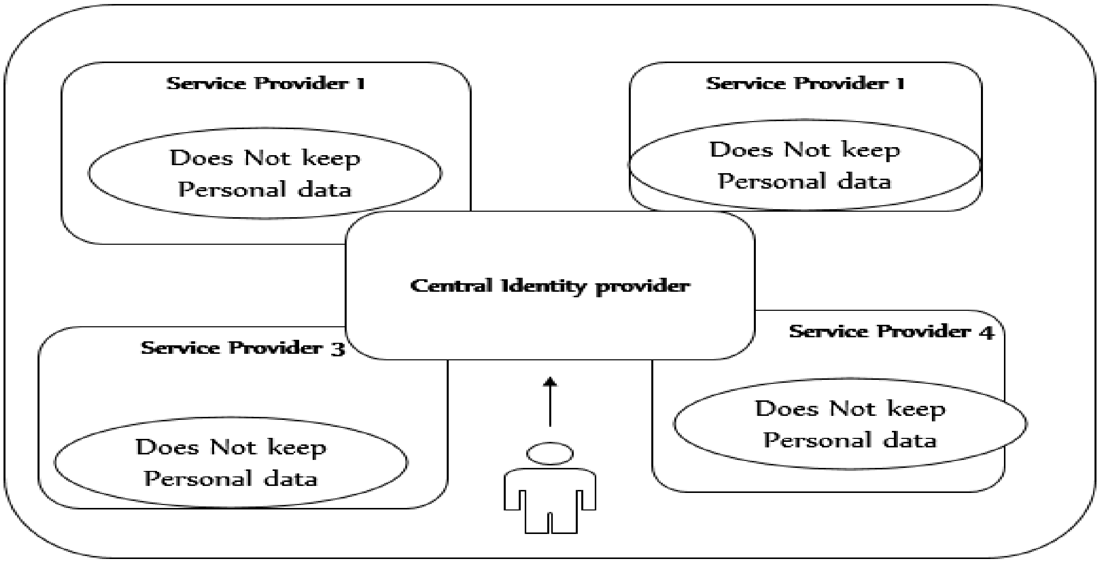

Service Provider 1
Does Not keep Personal data
Service Provider 1
Does Not keep Personal data
Central Identity provider
Service Provider 3
Does Not keep Personal data
Service Provider 4
Does Not keep Personal data

Figure 2.Centralized Identity Management Model [12]

2.3.3 Federated Identity Systems

FIM can be seen as an extension of distributed identity management across the organization's borders to facilitate the secure sharing of resources, processes, and technologies related to identity management in a heterogeneous environment [22]. A federation is defined as an association based on the trust of multiple organizations that collaborate to share resources or services[14]. FIM is a collaboration among one or more relying parties and identity providers to share user identity information such that a user from one organization can authenticate itself to another organization in the federation using the identity credentials from its organization and then gain access to other organization's shared resources or services [20].

FIM can be implemented in a centralized manner where one IDP is responsible for user registration, and authentication and all other RPs rely on the authentication assertions from the IDP. The other approach is to have a distributed architecture where each collaborating organization maintains a local repository of user identity information and performs authentication locally but supplies authentication assertions for distributed services across company borders [18][22].

Federated IdM seems to be the appropriate approach for handling authentication and authorization in a cooperative autonomous system where each local system has its IdM with independent identity schema and with the ownership of the identities it possesses. Permissions to release personal information in the cooperative system are governed by agreements done among the different organizations and these agreements are trust relationships that form the “circle of trust” in the cooperative system[2].

However, if the identity provider chooses not to establish a federation relationship with users’ preferred service providers, users may be unable to use their federated accounts to access those service providers. Another challenge relates to the problem of determining liability for these complex business relationships and protection against theft and errors. The main vulnerabilities stem from the fact that the identity provider knows which identifiers correspond to a given user. Thus, such knowledge places the identity provider in a position where it could impersonate the user or enable others to do so[19].

FIM is considered a promising approach to facilitate secure resource sharing among collaborating partners in heterogeneous IT environments. FIM is about inter-organization and inter-dependent management of identity information rather than identity solutions for internal use, and that it has emerged with the recognition that individuals frequently move between corporate boundaries. The federation model enables users of one domain to securely access resources of another domain seamlessly and without the need for redundant user login processes [23][20].

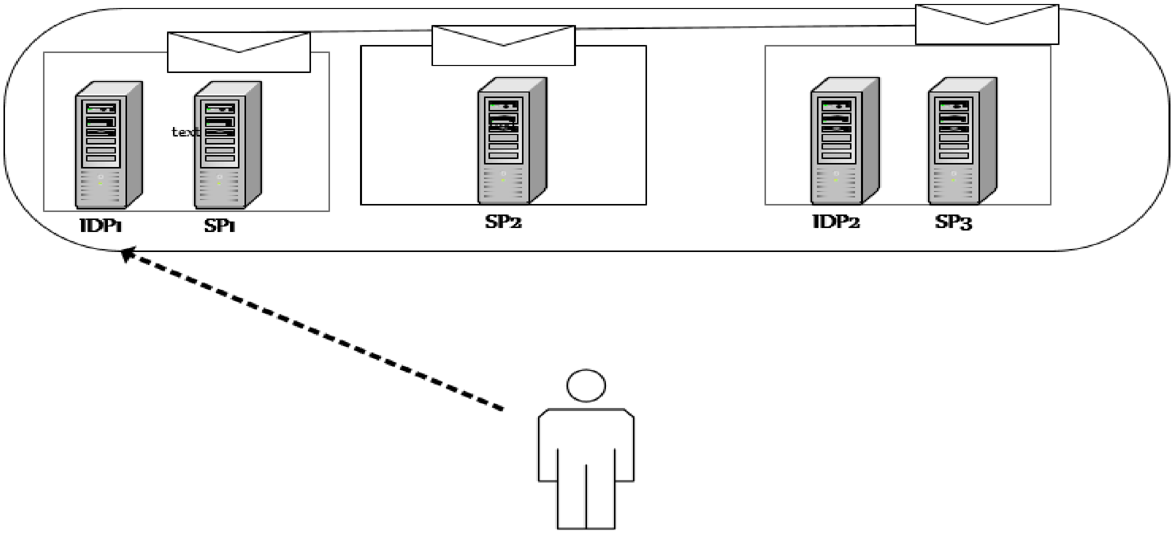


Figure 3. Federated IDM [19]

2.3.4 User-centric identity systems

User-centric IDMS seeks to offer users the flexibility to choose identity providers independent of service providers, and do not necessarily need to provide personal information to potential service providers to obtain access to services and resources. In such a model, the roles of Identity providers is that of a trusted third party who store user account and profile information and authenticate users, and service providers accept assertions or claims about users from the identity providers[21].

The user-centric model is also designed to ensure that identity providers operate in the interest of the users rather than in the interest of the service providers. In a user-centric model, service providers and identity providers do not necessarily form part of an identity federation. Thus service providers merely become “relying parties” with users being able to choose what information to disclose when dealing with service providers in particular transactions. The identity providers work as a third trusted party between the users and the service providers mainly targeting the interest of users [19][21].

2.4 E-Government in Ethiopia

According to the study [5], e-government has 5 stages of development which indicate the country's level of e-government development.

- **Emerging stage**. A government‘s online presence comprises of a web page and an official website. There is little interaction with citizens and information is static.
- **Enhanced stage**. Governments have created links to archived information that is easily accessible to citizens e.g. documents, forms, laws, and regulations, etc. There is more information on public policy and governance.
- **Interactive Stage**. There is a basic interactive portal with services to enhance the convenience of citizens. Governments deliver online services such as downloadable forms for tax payments and applications for license renewals.
- **Transactional stage**. Governments begin to transform themselves by introducing two-way interactions between citizens and government. It includes options for paying taxes, applying for ID cards, birth certificates, passports, and license renewals. All transactions are conducted online.
- **Connected Stage**: Governments transform themselves into a connected entity that responds to the needs of its citizens by developing an integrated back-office infrastructure. It is characterized by vertical and horizontal G2G connections, G2C, G2B, and infrastructure connections.

2.4.1 Identification System and Vital Registration in Ethiopia

The legal basis for the national ID as well as for the establishment of a civil registration system is Proclamation No. 760/2012: “A Proclamation on the Registration of Vital Events and National Identity Card.” The proclamation motivates the national ID project by noting that: “the issuance of national identity cards to citizens has become important for the protection of national security, and for providing efficient services to citizens by the public and private sectors.” It states that the National ID is to be managed by “an appropriate Federal Organ” Which is the National ID agency. Implementation was originally scheduled for July 1, 2016. However, unlike vital events registration agency, the agency has not been organized since the necessary regulations have not been issued. It falls under the jurisdiction of the Information Network security agency, INSA [24]. The National ID Agency (NIDA), is responsible for enrolling all Ethiopians over the age of 17 into a national database and issuing to them a national ID card and the Vital Events Registration Agency (VERA), is responsible for civil registration and vital events. The two forms of identification implied by this proclamation—the birth certificate and the national ID—are to be linked with a unique national ID number to be issued by the NIDA and included in the birth certificate issued by VERA [24]. The national ID card will include the attributes full name including grandfather, sex, date, and place of birth, principal residence, photograph, fingerprint [24].

The Ethiopian governmental structure consists of a federal government divided into 9 autonomous regional states and two city administrations with individual administrations [24] [25]. It follows a decentralized administrative system where the regions have legislative, executive, and judicial powers. The organizational arrangement for each regional agency follows the decentralized administrative structure[24]. The states are divided into several sub-cities, which are again divided into approximately 800 Woredas, the district administrations, which are again divided into approximately 15000 Kebele offices, the local administrations [25].

Currently, in most parts of Ethiopia manual ID system issued at Kebele level is used for citizen identification. The kebele cards given in different regions have differences in citizen profiles content, language, card color, and type. The citizen's Unique ID number is valid only for the kebele the citizen first takes the card, if the citizen moves to another kebele or woreda he/she takes another ID number [25]. Although some efforts are made to introduce e-governance in the country, no significant effort is made on the Citizen Identification System, which can greatly assist e-governance by enabling the sharing of individual citizen information to facilitate the service rendering process of government offices.

2.4.2 Taxpayers Identification Number in Ethiopia

For tax collection, the Federal Revenue Authority (FRA) has started to use an integrated database system called Standard Integrated Government Tax Administration System (SIGTAS) that helps to identify Tax Payers by issuing Taxpayer Identification Number (TIN) in addition to customers fingerprint. This system is currently being used to uniquely identify only taxpayer organizations and businesses at all levels of the country. Moreover, the Authority is also working to expand the use of TIN to individual taxpayers but not the rest of the citizens [26].

2.4.3 National e-service portal

The Ethiopian national sService system is designed to provide a common platform and generic tools for online transactional services. Using the system, government organizations render electronic public services to citizens, non-citizens, businesses, and governmental and non-governmental organizations [27].

To file a service request, a citizen should log in using his/her account or can register to the system to get a user account and continue with his/her application. After locating the electronic form for a particular public service, the citizen fills out all mandatory fields, uploads documents, and submits the request after reviewing for error correction. After the submission of a request, the system generates an automatic application reference number for the citizen to track their application status[27].

To keep the privacy of users, User's personal information is available only to the government employees who need to know it. It will not be available for public inspection without user consent. Also, no site user information will be shared, sold, or transferred to any third party without your prior consent. Access is given only to those qualified professionals who provide Ethiopia Government services consistent with your interactions with our site[28].

The main question here is how will we manage identities of online service users? Can a citizen get access to services with no physical presence at the organizations? Can anyone steal a portal login account and apply and get a service? can the portal connect at the back organizations vertically and horizontally? Is the portal scalable to the stage V E-government development stage? These are some of the critical questions that the implementation body would have to answer in identity management.

2.4.4 ICT Infrastructure in Government Agencies

The ICT infrastructure is one of the major activities which is to be available, at least on the minimum level. The infrastructure includes multiple components, some of them are the telecommunication infrastructure, the different level of e-Government data centers, the different level of networking, the servers, computers, etc. [29]

Woreda-Net is one of the public network infrastructure established purely to link administrative components to make the government operations transparent, to make the government accountable, to increase citizen participation in government[29][30]. In this virtual private network over 630 Woredas are connected and getting services indicated above. In connecting those Woredas, one National Data Center and eleven regional data centers are established. The connection is through a combination of terrestrial and VSAT type. In the physical connection, more than 4,000 KM is optical fiber cable [29][30].

2.4.5 **Types of Interactions in E-Governance**

The flow of information between the Government and Citizens, Government and Businesses and Government and Government is referred to as Governance. E-Governance also covers all these relationships as follows[31][32]:

- **G2G (Government to Government)**: When the exchange of information and services is within the periphery of the government, is termed as G2G interaction. This can be both horizontal, i.e. among various government entities and vertical, i.e. between national, state, and local government entities and within different levels of the entity.
- **G2C (Government to Citizen):** The interaction among the government and the general public is G2C interaction. Here an interface is set up between government and citizens, which enables citizens to get access to a wide variety of public services. The citizens have

the freedom to share their views and grievances on government policies anytime, anywhere.

- **G2B (Government to Business):** In this case, the e-governance helps the business class to interact with the government seamlessly. It aims at eliminating red-tapism, saving time, cost, and establish transparency in the business environment, while interacting with government.
- **G2E (Government to Employees):** The government of any country is the biggest employer and so it also deals with employees regularly, as other employers do. ICT helps in making the interaction between government and employees fast and efficient, along with raising their level of satisfaction by providing perquisites and add-on benefits.

2.5 The Identity Ecosystem in Different Countries

To review the identity management system implementations in different countries, choosing a country that has a good balance in terms of geography, population size, and layers of government, diversity of cultures and styles of government should be ensured [13]. We have selected 2 countries based on two main criteria's, the first criteria is a country which has similar characters with Ethiopia by the number of population, culture, and political structure. The second criteria are countries that have implemented recently and best experience in digital identity management. Based on the first criteria we have selected India and from best-experienced countries Australia.

2.5.1 India

India's eIdM project which is named Aadhaar project is the world's largest national identity project, launched by the government of India, which seeks to collect biometric and demographic data of residents and store these in a centralized database. At its core, the Aadhaar act attempts to create a method for the identification of individuals to provide services, subsidies, and other benefits to the residents of the country. Even more importantly, Aadhaar can facilitate linking of local ids in currently isolated verticals like census, education, health-care and immunization records, birth, and death records, land records, property registration, income tax, banking, loans and defaults, police verification and law enforcement, disaster management, security and intelligence, and such others[33][34][24]. Enrolment in Aadhaar requires the collection of ten fingerprints, two iris images, and a digital facial photograph, along with basic biographic data (name, date of birth, sex, and address). Once these four requirements have been met, a randomly generated number is given to the user. Unlike other systems, including Estonia's, there is no physical credential that is provided as a result of signing up for Aadhaar. Instead, all authentication is done using biometrics[34].

The key components of the Aadhaar system include the following:[34]

Enrolments Software: The enrolment software, owned by UIDAI, captures demographic information and biometric data with the consent of the user obtained at registration. The software then securely transmits that information to the Aadhaar system.

CIDR: The Central Identity Repository system stores the demographic and biometric data after issuance of the Unique ID number (Aadhaar number).

Aadhaar services/APIs: Unique Identification Authority of India (UIDAI) has open APIs to allow service providers in the public and private sector to authenticate users based on one or more of the following: biometrics, demographics, and One Time Password (OTP) on registered mobile phones. The service providers must register as Authentication user agency (AUA)/ sub AUA with UIDAI and access the APIs via the ASA (Authentication service agency).

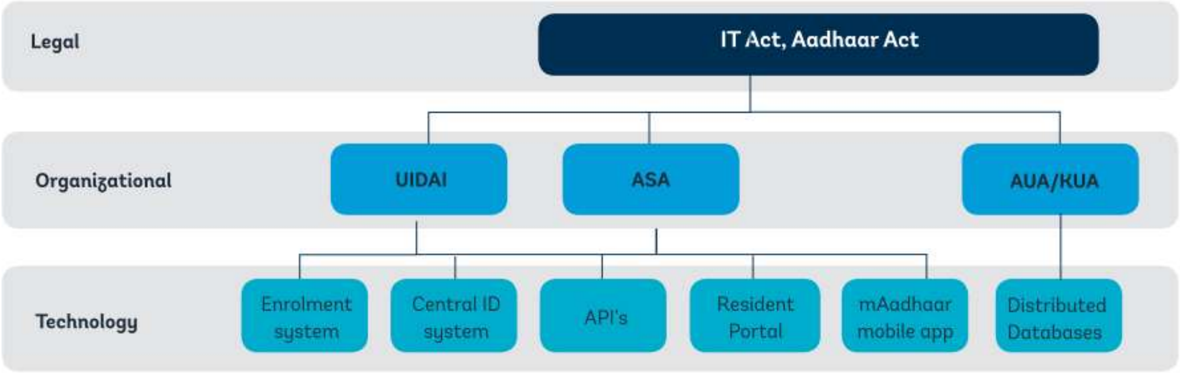


Figure 4. Components of Aadhaar System [32]

In 2015, the Government of India has prepared an interoperability framework for e-governance (IFEG) to deliver services to citizens by ensuring Interoperability amongst various e-Governance systems and applications. Without the assurance of interoperability, citizens will have fragmented interactions with several agencies [35].

2.5.2 Australia

The first Australian Government Authentication Framework for Businesses and Australian Government Authentication Framework for Individuals (AGAF-B and AGAF-I) was developed in 2003 and then the Australian Government Information Management Office (AGIMO) has developed The National Authentication Framework (NeAF) in 2009 by replacing the earlier. The framework aimed at achieving consistency by providing guidance and principles, trust and confidence, cost-effectiveness and convenience, "fit-for-purpose authentication solutions" for individuals, businesses and government websites, responsiveness and accountability, privacy controls, and interoperability based on federation [13].

In 2019, The Australian Digital Transformation Agency (DTA), in collaboration with other government agencies and key private sector bodies, is leading the development of a national user-centric federated digital identity system (the 'identity federation'). Implementation and operation of the identity federation are underpinned by the Trusted Digital Identity Framework (TDIF)[36]. Since it is user-centric IDM, first the government accredited People can choose their digital identity and credential service providers from a range of accredited government and private sector providers [36]. A unique citizen identification number is not required to get the services provided by the service providers, instead, the user can use any ID from an identity provider he/she chooses. A “trust framework” describes a legally binding and agreed set of specifications, rules, and agreements for the governance of a federated identity system established to enable participants to have confidence in the functionality and trustworthiness of federated identity systems [36].

The Australian TDIF includes different requirement documents for the implementation of a user-centric federated digital identity system. Main requirement documents are privacy, security, technical, architecture, attribute, and OpenID 1.0 and SAML 2.0 profiles[37][36].

2.6 Existing Protocols and Standards

2.6.1 OpenID 2.0

The OpenID 2.0 [38] family of specifications were designed to be a much simpler (but also less flexible) FIS scheme compared to SAML. The simpler protocol message format enables OpenID-based IdPs and SPs to communicate without requiring prior agreement on a large set of protocol parameters as was the case with SAML. The design philosophy of OpenID was to allow any domain owner to set up an IdP (users can, therefore, set up their own IdP if desired) and provide services to any SP without prior coordination. OpenID SPs experimented [39] with various user interface designs for obtaining users' OpenID identifiers generally, users would select their IdP from a list of logos of the most popular IdPs and subsequently type in their user name (the SP could then determine the correct IdP URL corresponding to the user name); more advanced users could pick the option to manually enter their URL instead (e.g., if they host their own IdP or use a lesser-known IdP).

2.6.2 Security Assertion Markup Language

SAML is an XML-based framework developed by OASIS for communicating user's information related to authentication and authorization[40]. It permits the two federated partners to select and share the necessary identity attributes they require in a SAML message/assertion provided that they can be represented in XML [41].

2.6.3 OAuth 2.0

OAuth 2.0 is an authorization protocol for gaining access tokens for web APIs and secure resources. OpenID Connect relies on the OAuth 2.0 semantics and streams to permit applications to admit users[42].

OAuth 2.0 structures, which are defined by the Internet Engineering Task Force (IETF) in RFCs 6749 and 6750, became available in 2012. These structures were intended to support the improvement of authentication and authorization protocols. They provide an assortment of standardized information flows that depend on JSON and HTTP.

OAuth 2.0 [43] authorization structure allows a third-party (e.g. an RP) application to gain partial access to an HTTP service, either on behalf of a resource owner by coordinating an agreement communication between the resource owner and the HTTP service or by permitting the third-party application to gain access on its behalf.

2.6.4 OpenId Connect

OIDC is an identity layer built on top of the OAuth 2.0 protocol. The OIDC uses RESTful HTTP APIs and JSON data format. Most of the specifications in OAuth 2.0 apply to also to OIDC. This also means that the OIDC specification has most of the OAuth 2.0 capabilities integrated into the protocol. It allows clients to request and receive information about identities and currently authenticated sessions. The specification also allows encryption of identity data, the discovery of OpenID provider, and advanced session management, including log out. [44][45].

There are already more than half a billion user accounts based on OIDC with OP being Google, PayPal, and Microsoft [46]. OIDC has been built based on the experiences from the existing protocols and solution and with the underlying principle to keep simple things simple and to make complicated things achievable in an as simple manner as possible. Simplicity has been the major focus in OIDC design so that developers can integrate it more easily and efficiently compared to preceding protocols such as SAML or OpenID [47],[48].

OIDC also has the capabilities to fulfill the requirements of the federated identity management at the enterprise or academic level as done by SAML today but in a much simpler manner. It also stresses on the fact that although SAML protocol is a very mature and robust protocol, it is quite a heavy protocol due it underlying XML and SOAP technology whereas JSON and REST are lightweight technology [48], [47].

2.7 Security Issues of IdM protocols

2.7.1 Man in the middle attack

A man in the middle attack is possible in OIDC when the OIDC client registration process happens. For registering a new OIDC relying party at the Authorization Server, the relying party sends an HTTP POST message including its metadata to the Client Registration Endpoint with a content type of application/JSON, and the parameters represented as top-level elements of the root JSON object. The subsequent response may carry a Registration Access Token, which can be used by the relying party to accomplish required tasks upon the resulting registration. The OIDC identity provider may require an Initial Access Token to limit registration requests to only authorized clients or developers [49]. However, to support an open dynamic registration, the Client Registration Endpoint should accept registration requests without OAuth Access Tokens. Therefore, the dynamic client registration could be the potential source of many attacks including the man in the middle attack[41]. The man in the middle attack may be caused by a logical flaw in the OAuth protocol or the presence of a malicious OIDC identity provider or malicious relying party [50].

When the service provider Initiated single-sign-on (POST) message flow is requested, there's a chance of man in the middle attack in SAML. This exchange uses a POST binding for the service provider-to-identity provider authentication Request message associate an artifact binding for the identity provider-to-service provider Response message [50]. Additionally, SAML service provider-initiated single-sign-on (POST) process, the SOAP binding is used which is vulnerable to the man in the middle attack[51]. The Relay State token is not a transparent reference to state information that is maintained at the service provider. This Relay State mechanism can leak information about the user’s activities at the SP to the identity provider if the service provider deployment is erroneous or some other kind of existing vulnerabilities which may also lead to the man in the middle attack [52].

2.7.2 Cross-site scripting attack

As stated in [46], cross-site scripting attack in OpenID Connect(OIDC), an attacker exploits the facility of an automatic authorization granting by which an automatic authorization response is created if a user had recently a session with the OIDC identity provider and previously granted authorization for the same client. Using this facility, an attacker may be able to steal a user access token by exploiting cross-site scripting vulnerability on the client-side. Naik and stein [41] state that as this vulnerability is revealed in Android's built-in browser has been exploited for this cross-site scripting attack. Where an attacker utilizes a browser window. Open event for sending a counterfeit authorization request to the OIDC authorization server, in which response type=code is altered to response type=code token id token.

The study [53] indicated that exploitation of the vulnerability of the erroneous deployment of SAML framework assists an attacker to perform progressively tricking a user by visiting URIs that may be vulnerable to cross-site scripting attack. This is a quite severe cross-site scripting attack since the client is not suspicious of receiving an altered resource and a Response used in the SAML process could contain unencoded data supplied by an untrusted source. In the end, an attacker uses data to start a cross-site scripting attack by redirecting a user to a maliciously crafted URL. Besides the issue of SAML Response, a basic deployment of SAML exposes the Relay State field to a probable injection of malicious code which may be executed at the honest service provider side[41].

2.7.3 Denial of Service Attack

SAML provides two common message flows, service provider-initiated and identity provider-initiated, and the two common messages SAML provides are an Authentication Request message sent from Service provider to an identity provider, and a Response message, containing a SAML assertion, sent from the identity provider to the service provider[54], [41], [55].

Service provider Initiated Single-sign-on (Redirect/POST Bindings) message flow can cause a denial of service attack in SAML. Thus, the user is sent to the identity provider to log on and the identity provider delivers a SAML web single-sign-on assertion for the user’s federated identity to the service provider. This exchange uses a Redirect Binding for the service provider-to- identity provider Authentication Request message and a POST binding for the identity provider-to-service provider Response message. Here, an attacker can target the identity provider by sending an abundance of requests by compromising valid users or an honest service provider because the SAML request requires substantial processing overheads [55].

OIDC identity provider configuration information is necessary for the OIDC discovery process. The OIDC identity provider allows metadata discovery and therefore, it hosts its configuration information at the endpoint. In most of the implementations, the endpoint is accessible by any client/RP who is wishing to send registration request and thus, it is publicly open and possibly non-secure. Subsequently, OIDC client sends an HTTP GET request to this metadata endpoint to obtain the configuration information of the OIDC identity provider. The OIDC identity provider sends a response which is a set of Claims about the OIDC provider's configuration, including all necessary endpoints and public key location information that can be used by client/RP for further communication with the OIDC identity provider or the OAuth authorization server[41].

A denial of service attack in OIDC is possible when the endpoint is publicly open and non-secure, and the dynamic discovery process is allowed without any authentication. This vulnerability can be easily exploited for the denial of service attack on an OIDC identity provider and flooded by countless dynamic discovery requests, which could easily overwhelm the OIDC identity provider [55].

2.8 Comparison of IAM protocols

The features, merits, and limitations of SAML, OAuth, and ODIC standards are analyzed in the previous section. OIDC and SAML are a complete solution for both authentication and authorization, though OAuth used for only authorization.

Business models- enterprise-to-enterprise, enterprise-to-consumer, or within an enterprise may have specific authentication and authorization requirements. A large division of the current users of the web and mobile communications market is associated with both enterprise users and consumers. Therefore governmental IAM standards should provide support to government-government and government-public user's authentication and authorization. To integrate Fragmented government systems around the country using enterprise and consumer level identity and access management technologies is better for public service delivery [41].

The literature [41] has pointed out the major architectural difference between the two protocols. The architectural design of SAML requires enterprise service provider and enterprise identity provider, and a reliable relationship, therefore, it is mostly suitable for enterprise-to-enterprise users. While, OIDC design is also focused on end-users and, therefore, it is suitable for both enterprises and consumers and all business models in case of untrusted third party association.

Identity and access management standards should be lightweight and secured to better suit for both web and mobile applications. Applying data compression to remove unnecessary data reduces the size and network traffic[56][57]. SAML is an XML-oriented specification and the representation of XML trees is quite wordy, and every element of a tree is surrounded in a pair of tags with its element type. Whereas OIDC is a JSON-oriented specification and the representation of JSON trees is less wordy than XML as it is in the form a nested array type analogous to that of JavaScript. Therefore, the more compact size of OIDC makes it the preferred choice for communication in HTML and HTTP environments than SAML [58].

In the current web technology, security is always a great concern. Due to insecure channels, the web is more disposed to snooping attacks[59]. The protection of security tokens which should not be tampered with or altered during its entire life cycle and confidential information should be protected from revelation to unauthorized users. These two security provisions can be maintained by strong encryption techniques and digital signatures or MAC should be incorporated in identity and access management standards. SAML XML tokens can be signed using XML Signature (XML-Sig) based on a secret key using the HMAC algorithm or a public/private key pair in the form of an X.509 Certificate. In practice, SAML tokens are generally signed with a private key because of the established relationship between the identity provider and service provider. SAML XML token data can be encrypted using XML Encryption based on a secret key (Triple-DES-192, AES-128) or public/private key pair (RSA-PKCS1-1.5-192, RSA-OAEP- 128/256). However, signing a part of the message, creating an overlapping signature, and adding or subtracting text after signature features make it vulnerable for many new security threats. Furthermore, computing and verifying XML signatures are very resource-intensive [60][61].

JSON Web Signature (JWS) based on a secret key (with HMAC algorithm) or a public/private key pair (in the form of an X.509 Certificate) can be used to sign OIDC JSON Web Tokens. OIDC JWT data can be encrypted using JSON Web Encryption (JWE) based on a secret key (AES-128-CBC, and AES-256-CBC) or public/private key pair (RSA-PKCS1-1.5-2048, ECDH-ES-256). However, some JWT libraries treat tokens signed with the none-algorithm as a valid token with a verified signature, which allows arbitrary account access on some systems [62]. SAML and OIDC both offer strong security features. However, comparing signing JSON with XML, the complexity of signing XML with XML Digital Signatures may leave some security holes [58]. According to [41], JWT does not use sessions while SAML does; which prevents OIDC from many attacks related to sessions including Cross-Site Request Forgery (CSRF), thus, OIDC is more secure for web and mobile applications.

Different identity and access management protocol comparison studies have conducted in the previous years. In [63] the researchers compared and implemented security investigations on three SSO protocols namely LDAP, SAML, OpenID, and concluded that the LDAP protocol was designed for local networks, not web requests, and that SAML is out of date and is no longer use for web requests. In[64] Sun proposes improvements to enhance the security of a web SSO system. He illustrated that though OpenID and OAuth have been approved via IdPs, including Google, Facebook, Yahoo, and Microsoft, as well as millions of RP websites, the normal user still poorly understands web SSO. Sun concluded that users need to advance their understanding and that enhancements to usability and security would assist them in doing so. In[65] the researchers' studies on Integrity, Availability, and Confidentiality of OpenID IdPs for Information and Process and concluded that OpenID identity providers could achieve good throughput, and are appropriate to support thousands of users.

	Criteria	OIDC	OAuth	SAML
1.	Authorization and Authentication	It is a standard for both	It is a standard for only authorization	It is a Standard for both
2.	Main purpose	Identity & Access Management, single-sign-on for both enterprise and end-user	API authorization	Identity and Access Management, single-sign-on only for enterprise
3.	Token format	JWT ,JSON	JSON, JWT, XML	XML
4.	Token content	User identity information without credentials.	User identity information without credentials	User identity information without credentials
5.	Lightweight standard	Lightweight standard, due to JSON has a much smaller grammar and maps.	Lightweight (JSON states trees in a nested array type of notation similar to that of JavaScript)	not lightweight standard (XML states trees in a verbose form)
6.	Protocol used	JSON, HTTP, REST	JSON,HTTP,REST	XML,HTTP,SOAP
7.	Platform Independent/Vendor-Neutral/Open Standard	Yes. Uses Standardized parameters like instance scopes, endpoint discovery, and dynamic registration of clients (implementers task in OAuth 2.0)	Yes. Have different design models due to its flexibility in the Implementation	Yes. Have different design models due to its flexibility in the Implementation
8.	Web and Native Mobile Apps support	Yes	Yes	It is specially designed for web apps. However, HTTP artifact binding can be used to reduce the flow
9.	Enterprise and consumer support	It supports enterprise users, and consumer apps and services (IdP, RP, and SP).	It supports enterprise users, and consumer apps and services (IdP, RP, and SP).	Since it involves only SP and IdP, mainly supports enterprise users.

Table 4.1. Comparison of common IdM Communication protocols as of [41]**,**[3], [18], [64]

2.9 Identity Management & Privacy

Different countries may have different privacy principles based on their data privacy policies, I.e. EU Data Protection Directive lays down certain privacy principles to manage personal data which are also relevant to enterprise FIM. The most common data privacy principles as of [66] [67] are:

- Fairness and Lawfulness – handling of data should be lawful and fair?
- Finality - data collection and processing must be limited to specific legitimate purposes?
- Proportionality - only collect minimum data that is required for the purpose; no excessive data collection
- Data Quality - data must be accurate and recent; any incomplete, inaccurate data must be rectified
- Information Security - confidentiality and integrity of data must be preserved at all times?
- Openness and Transparency - policies regarding data collection, processing, and storage should be clear
- Individual Participation - an individual has the right to obtain his/her data as available with the data controller within a reasonable time and in a readily intelligible format.
- Accountable - the data controller is responsible for upholding the above principles.

E. Birrell and Fred B. Schneider [3] have stated three basic privacy principles for identity management?

- Undetectability of Authorization Requests - this involves hiding user actions from the identity provider. An IdP should not be able to detect the context and the SP to which the user wants to forward the identity assertions. Credential based assertions provide such feature. Credential based assertions are transferable, and once it is issued to a user, the user can forward the assertion to SPs without the involvement of IdP. The opposite approach that provides non-repudiable linkability the interactive approach where the SP and IdP actively communicate and identity assertions are exclusively released for a specific context and a specific service provider. This interactive approach provides detectability and also allows the identity provider to control the release of specific attributes to specific service providers.

- Unlinkability - this privacy property refers to avoiding the co-relation between the actions and identities. Decentralized IdPs where each IdP is only responsible for specific attributes and each function independently of another can provide unlinkability. To restrict an SP from linking actions to identities, the IdP can issue a new unique identifier each time an authentication request is made. On the other side, if linkability is desired then a centralized IdP should maintain user identity attribute and must provide the same identifier per user per SP to maintain the linkability of actions and identities.
- Confidentiality - Identity management should allow the users to control which identity attributes should be revealed to which service provider. Users should have the ability to save their permissions for each service provider or should be able to define policies for the release of attributes.

2.10 Summary

In this chapter, we have discussed the different approaches to implement identity management systems, the existing communication protocols, and security issues during identity management implementations. It is necessary to identify the main purpose of IDM systems, the administrative issues, and technical issues, and then the government adopts the legal standards before implementing it.

Findings:

- The IDM implementation model based on legislation adopted by the government bodies which depends on the existing trusted identity providers in the country, the goal of the IDM implementation, and administration structures. In the adopted government legislation, if the citizens have the right to select from a list of trusted identity providers chosen by the government to access services, the user-centric identity model is a better solution.
- For those countries in which the government is both the identity provider and service provider to integrate and share the resources from distributed and fragmented systems, federated identity management model is the better choice.
- Using the National ID as a platform for public eService delivery is the best practice in different countries.
- To use identity systems for public online service delivery, the government should assign different implementation bodies at the organizational level such as national ID, PKI or authentication and authorization and vital events, etc.
- Implementation of identity management systems needs different rules and regulations to fulfill minimum requirements to act as IDP, SP, Client, and user.
- OAuth has very good characters to fulfill modern web and mobile requirements. It is suitable for only authorization but not for authentication. SAML most widely used for enterprise IdM systems implementation, but it is not recommended for consumer-

level services due to the complexity of long XML trees. OpenID Connect has better features for both enterprise-enterprise and enterprise to consumer identity management systems. OIDC is a JSON based lightweight protocol suitable for both web and mobile communications.

- OIDC is less vulnerable to security threats compared with SAML which exposed to modern security threats due to its session and signing a part of a message during communication. Though IDM technologies have a high-level security feature, no protocol is fully secured alone without additional security features. So, to implement secured IDM technology designing a security framework that fulfills the privacy and data protection standards is necessary.

Chapter 3

3.1 Methodology

Within the IS domain, design science is a problem-solving approach that aims to develop a practical solution to a common problem to improve the IS development or management process. This process involves critical thinking and innovation to resolve the problem at hand by the creation and application of the designed artifact. Design Science Research in the IS domain must result in a practically useful artifact that solves an important and complex business problem [68].

This research aims to design an implementation framework of cross-organizational identity management with suitable interoperability, integration, and security protocol. The research involves designing practice to improve the current practice of fragmented public sector systems to become interactive and interoperable for data access and sharing in the context of the Ethiopian e-government model concerning the Ethiopian identity policy, legislation, culture, and existing infrastructure. Therefore, one of the most appropriate research methods to carry out this research is the design science research method.

3.1.1 Design Science Approach

This research has been planned according to the main activities involved in design research. Van der Merwe, Alta Gerber, and Aurona [68] and [69] have identified the most common steps to conduct research using design science approach :

1. Explicate Problem – An iterative process to study the existing knowledge base to get a clear understanding of the problem at hand and possible approaches to the solution.
2. Define requirements – This involves further analysis of the problem to create a clear set of requirements that must be fulfilled to resolve the problem. The requirements define the features that the solution artifact must have within the constraints of the environment in which it will be used.
3. Design & Develop artifact – This phase involves building the actual artifact based on the requirements and knowledge gathered in the previous two phases.

4. Demonstrate Artifact – In the phase, the developed artifact is practically applied to one or more problem instances to demonstrate its usability and usefulness.
5. Evaluate Artifact – In this phase, the developed artifact is critically evaluated to measure the degree of achievement of the requirements set in the requirement phase. Evaluation can be either qualitative or quantitative.

Business needs from the environment can stem from people, technology, or organizations. In the center are the activities related to development, building, and evaluation of the new artifact. The contribution is both backs to the environment in the form of an artifact with practical value and rigor in the form of new knowledge[68].

3.1.2 Research Strategy

There are many research strategies to gather requirements. Case studies[70] are used to conduct a detailed investigation of the requirements from various stakeholders such as the identity provider, relying- parties (government organizations), the end-user (government employees) and customers of the organizations. However, case studies require many resources, time, and competence from the researcher to conduct the case study in an unbiased manner; moreover, it is difficult to find and get the requirements in Ethiopia since there is no local identity provider. Another research strategy that could be used is survey [70] where the questionnaires are created either online or offline for each type of stakeholder – identity provider, relying party and end-user, and then requirements are discovered from the response of the survey questionnaire. Surveys are comparatively easy to conduct than case studies. However, they are limited in their ability to gain insightful requirements, stakeholders may be biased or may be reluctant to reveal detailed information and they may also miss important requirements. For this research, we choose physical observation at the service providers and documents study [70] as the method for requirements gathering. During our observation in the three regional organizations, we observed that- which type of technologies are they using? How do they provide customer services? How their organizational tasks are dependent on the other organization tasks? How do they share data? Document study involves a careful study of the existing relevant literature to collect requirements and get the experiences of other countries. It builds on similar works done previously and has the advantage of collecting requirements from different viewpoints of stakeholders and different scenarios. Identity management has been researched extensively so high-quality peer-reviewed articles were available to collect requirements. Therefore, document study was the most suitable additional method for requirement gathering.

3.2 Requirements

Among the five steps of the Design science approach stated in [68] and [69], the prerequisite for design and development of the implementation framework is to have identified a set of requirements that will guide the process of development. The evaluation and development of artifacts also depend on the defined set of requirements.

3.2.1 Initial Requirements

The initial set of requirements collected from the literature of identity management and studies on government national Id implementation. All these major requirements are independent of any technology, protocol, or framework or system.

Article [71] [72], have identified the basic laws of identity are very practical and the product of extensive discussion among the leading architects in the field of IDM. The major requirements selected by the article are-

- User Control and Consent - The user must be in control at all times of what identity information is revealed, to whom, and for what purpose [71]. The user must have the ability to choose whether to reveal identity information to a certain relying party [72].
- Minimal Disclosure for a Constrained Use - To moderate the risk of a possible data breach and compromising user's identity information, an identity management system should only maintain the least amount of information required for identification[71] [72].
- Justifiable Parties- identity information should only be disclosed to relying parties that have a valid reason to acquire that information. The user must be made aware of which relying party their identity is going to be revealed, and the relying party must state the policy statement on the use of the identity information [71] [72].
- Directed Identity - An identity management system should support Omni-directional identifiers for public entities that want to be discoverable by all e.g. a public website has a public URL and public certificate that is known to all. In the case of individuals, the

identifiers should be unidirectional so that the identity information is private. The use of different unique identifiers for a different service provider will prevent those service providers from correlating information about the user [71]. FIM should promote limited likability such that linking of identity data across different domains is not possible [72].

- Pluralism of Operators and Technologies - A user can have identities from different identity providers, and each of these identities is relevant in different contexts. For example, government digital identity for use when interacting with government departments, employee identity at work. In the identity eco-system, there will exist multiple identity providers run by different organizations offering different or even contradictory features. Therefore, an identity management system must support interoperability to work with different identity providers employing different identity technologies [71]
- Human Integration - The identity management system must ensure that the communication between the user and the system is clear, predictable, and simple to avoid identity attacks such as impersonation and phishing [71].
- Consistent Experience Across Contexts - The identity management system must offer a consistent experience to the user across different contexts and multiple relying parties and technologies [71].
- Always maintain the basic security goals of confidentiality, integrity, and availability of the identity data at rest and during transmission [72].
- Audit and Monitor –identity providers should monitor the actions of its users and usage of services of relying parties. This audit is necessary for billing purposes and to keep a check on the misuse of the resources by the users [72]. Ensure that user identities are immutable, unambiguous, traceable, and support non- repudiation [72].
- Development and maintenance feasibility – the effort required to develop and maintain a secure FIM should be cost-effective, must use existing technologies and standards, must require minimal changes to existing systems and should be maintainable in the long run [72].

- Separation of privileges – Defining different roles for the administration of the identity management system and user roles that access various services would prevent the risk of impersonation and ensure that each role has specific responsibilities and functions [72].

According to the World bank identity management for development (ID4D) group [13] have identified the main principles to the development of national digital identity framework from the study conducted in different countries identity management experiences. The identified IDM entities are

- **Vision and Mission**: Any entity interested in developing a National Digital Identity Framework should precisely define a vision setting the goals it aims to pursue, and a mission detailing how to reach said goals.
- **Comprehensiveness**: The National Digital Identity Framework should result from an all-encompassing understanding and analysis of the overall digital environment, taking into consideration the country's context, circumstances, and priorities.
- **Social Inclusiveness**: The National Digital Identity Framework should be developed in a way that its services can be provided to the entire community of users, with particular regard for weak individuals and minority groups.
- **Economic and Social Prosperity**: It should foster economic and social prosperity and maximize the contribution of digital to sustainable development and social inclusiveness.
- **Fundamental human rights:** The ID Framework should respect and be consistent with fundamental human rights and values.
- **Trust, privacy, and Security**: ensuring adequate safeguards for the privacy of users and guarantee the appropriate level of security for the information to gain a high level of trust among users and stakeholders.
- **Flexibility and scalability**: operating in a flexible and scalable manner and ensure that it can be promptly and efficiently modified or updated when necessary.
- **Interoperability**: should take into account the role of interoperability as the ability of different systems to talk to each other, exchanging information and queries.

- **Identity as a platform**: should foster the development of digital ID as a platform, so that users can plug it into any domain and use it.
- **The uniqueness of ID**: should ensure that people can get only one ID.
- **Robustness and future-proofing technology**: Technologies and systems described in the National Digital Identity Framework and used for the creation of Digital IDs should be robust and scalable, ensuring at the same time that they are future-proofed and do not get obsolete very soon.
- **Data quality**: The National Digital Identity Framework should be the base for other programs of national importance. Thus, steps must be taken to ensure data quality at multiple levels.

The specific privacy and security enhancing operational and technical controls adopted by an ID system will depend on context and other design choices [73]. The European Union and ID4D in [74],[34],[73] discussed the important categories of privacy and security technologies and strategies are:

- **Encryption**: used to protect the vulnerability of personal data to being accessed or intercepted and read by unauthorized actors during storage and when it is transferred [73].
- **Digital certificates and PKI**: Issued by Certificate Authorities (CAs) to facilitate secure electronic communication and data exchange between people, systems, and devices online[73].
- **Tokenization**: Tokenization substitutes a sensitive identifier (e.g., a unique ID number) with a non- sensitive equivalent (i.e., a "token") that has no exploitable meaning or value. This can protect privacy by ensuring that only tokens, rather than a permanent identification number or other, are exposed or stored during a transaction [34][74].
- **Platforms for personal access and control**: Individuals have the right to access and correct their data, and to monitor how it is being used by governments and third parties (and to hold these actors accountable for misuse) [74][34].

- **Tamper-proof logs**: Ensuring that personal data are only accessed by authorized users and for authorized purposes requires some method of tracking transactions and who has accessed the data and when [74].
- **Datacenter security**: using the necessary international standards to improve data center management, security, and access control, including ISO/IEC 27001 (information security management systems), ISO/IEC 22301 (business continuity management), and ISO/IEC 55000 (asset management).
- **Implementing a cybersecurity program:** Implementing a cybersecurity program to build the capacity of the ID authority to protect its assets and the capacity of the national cybersecurity agency to perform a supportive and enabling role. The program includes different activities (I.e. A legal framework on cybersecurity, a Sectorial cybersecurity strategy for the ID system, Cybersecurity foundations, Intelligence monitoring, detection and analysis, Prevention, Enforcement, etc.**)**[34]**.**

Identity systems may use two or more authentication and interoperability technical standards based on their security framework. Most Commonly used technical standards used to relate with the identity credential to be used for authenticating the user as identified in [75],[76] are:

- Biometrics (ISO/IEC 19794-5:2011 (Face Image) Image standard—multiple competing standards are in use for capturing face image (PNG, JPEG, and JPEG2000 in most of the systems while GIF/TIFF (proprietary standards) may be in use in a few). For fingerprint image (JPEG, JPEG2000, and WSQ) standards are in use[77][78].
- Biometrics (ISO/IEC 19794- 2:2011 (Minutiae))—Data interchange format—ISO standards for different types of biometrics like fingerprint, iris, and face are listed [78][77].
- Card/Smart Card (ISO/IEC 7816)—Different standards exist for the different types of card—card with chip and without a chip. Each identity system would select a card based on various criteria like cost, features. The standard to be selected depends on the category of the card used for the identity system[78].

- Digital Signatures (FIPS 186-4- DSS)—standards of digital signature for the identity systems[76].
- 2D bar code (SO/IEC18004:2015—Quick Response (QR) code)—the standards commonly used PDF417 and QR code[76].
- Federation protocols (Open ID connect, SAML v2—2005, RFC 6749/ OAUTH 2)—Open ID Connect and OAuth combination are being increasingly used for federation while SAML has been used extensively earlier [75][56][41] [54].

3.2.2 Requirement Processing

As indicated in [79] analyzing the requirements qualitatively is the next step after requirement elicitations. The initial set of requirements were carefully studied to derive concrete and specific requirements. These requirements were further analyzed qualitatively using a list of activities like, is the requirement necessary? Is the requirement consistent with the other requirements? Are the requirements complete? Is the requirement feasible? Is the requirement redundant?

The final step in requirement processing was requirement validation. In this step, the requirements were assessed to ensure that they are defined in a standard manner and represent an acceptable description of the identity management system that will be implemented during the development phase. The focus here was to answer the question "Have I got the requirements right?" The validation process involved getting the requirements reviewed[79].

3.2.3 Final requirements

Model

- There must be a simple and reliable process to disassociate a relying party from the federation.
- There must be a simple and reliable process to disassociate an employee from the identity provider.
- All-access to resources at the relying party must be denied as soon as the government employee credentials are revoked by the identity provider.

Privacy and Security

- Limit the purpose for which personal data are collected and used. Put in place proper measures to prevent user profiling based on the data volunteered.
- Identity providers must provide the user with the option to log out globally from all the live sessions with one or more relying parties in the federation.
- All communication related to identity exchange between the relying party and identity provider must be digitally signed using one of the standard digital signing algorithms to ensure integrity and non-repudiation.
- All communication related to identity exchange between the relying party and identity provider must be encrypted using one of the standard encryption algorithms to ensure confidentiality.
- Identity providers must share identity information only with relying parties with which they have established trust and are part of the federation.

Interoperability

- The identity management system must be interoperable with different relying parties employing different technologies using OIDC.
- Identity providers must use a standard way to communicate the metadata information about the user attributes within the federation that is understood implicitly by all the members.
- The identity management system must work with employees using different computing devices and at poor network bandwidth area.

Government framework requirements

- Defining specific goals of the IDM framework
- The IDM system should operate in a flexible and scalable manner and ensure that it can be promptly and efficiently modified or updated when necessary
- should foster the development of digital ID as a platform, so that users can plug it into any domain and use it
- identifying the suitable governance model
- Assigning the necessary implementation bodies at the organizational level such as national ID, PKI or authentication and authorization and vital events, etc.
- Identify and adopting the necessary rules and regulations to fulfill minimum requirements to act as IDP, SP, Client, and user.
- Implementing the necessary privacy and security requirements

3.3 Identity management framework development

The main objective of this thesis is to design an interoperable identity management framework to integrate and share data of fragmented government systems across ministries and agencies for better public service delivery. This framework is designed in the context of the Ethiopian government structure and legislation.

The implementation framework would include the necessary governance model, legislation, design or system architecture, communication protocols, and security requirements which are major components and the key decision points that must be considered.

The National Revenue Authority, Amhara vital events office and Trade bureau System implementation, organizational problems, and working procedures are observed physically and included in the framework.

3.3.1 Governance model

The national and regional governments have a primary role in this Digital Identity Framework, acting as Regulator and Identity Provider at the same time. Since the main aim of this framework is to integrate fragmented government systems both the relying parties and identity providers are government bodies. On one hand, its role as a Regulator implies providing guidance and control on the National Digital Identity Framework, producing specific laws, regulations, criteria, conditions, procedures, and controls for the management of digital identities. On the other hand, acting as an Identity Provider requires a direct responsibility in terms of operation of the digital identity lifecycle, from identity proofing to credential management, authentication of identities, integration with Service Providers, and revocation of digital identities.

3.3.2 Regulations or laws

The Ethiopian governmental structure consists of a federal government divided into 9 autonomous regional states and two city administrations with individual administrations [24] [25]. It follows a decentralized administrative system where the regions have legislative, executive, and judicial powers. This implies that regional governments could have their own identity management and data sharing legislations depending on their interest.

Identity management framework requires multiple legal acts and regulations on issues like data protection, privacy, and security, interoperability, administration, trust, and information sharing. In the Ethiopian context, Identity management systems will have two levels of legal act adoption, the first is between regional states and national governments, and the second is local or between agencies in the region which have a high level of trust and flexibility.

3.3.3 Design/Implementation architecture

Identity management implementation is a complex task. To implement government-owned IdM, It requires the participation of multiple government entities. For government structures like Ethiopia, in which regional governments are autonomous, using common Identity provider for both horizontal and vertical integration would have less trust and flexibility.

Due to the above reasons government-owned federated IdM the suitable model. The common characters for the proposed federated IDM framework in each region are:

- All the regions and the national government should have their identity providers and employee portal (Relying party).
- The identity information of the government employees must store at their own regional/federal IDP.
- Each governmental organization shares data based on the agreed national or regional authorization policy.
- All the service providers must use national ID as a platform
    - Unique identifier for all the people
    - Assigned and stored centrally at the national level
    - Integrated with Vital events to provide basic individual information
- The IDM system should be scalable and simple to implement online service delivery to the citizens.

- The IDM systems should use Biometric (Photograph) and federation protocol OpenID Connect for Authentication and Authorization.
- Vertical integration would be implemented using one common IDP and Common portal.

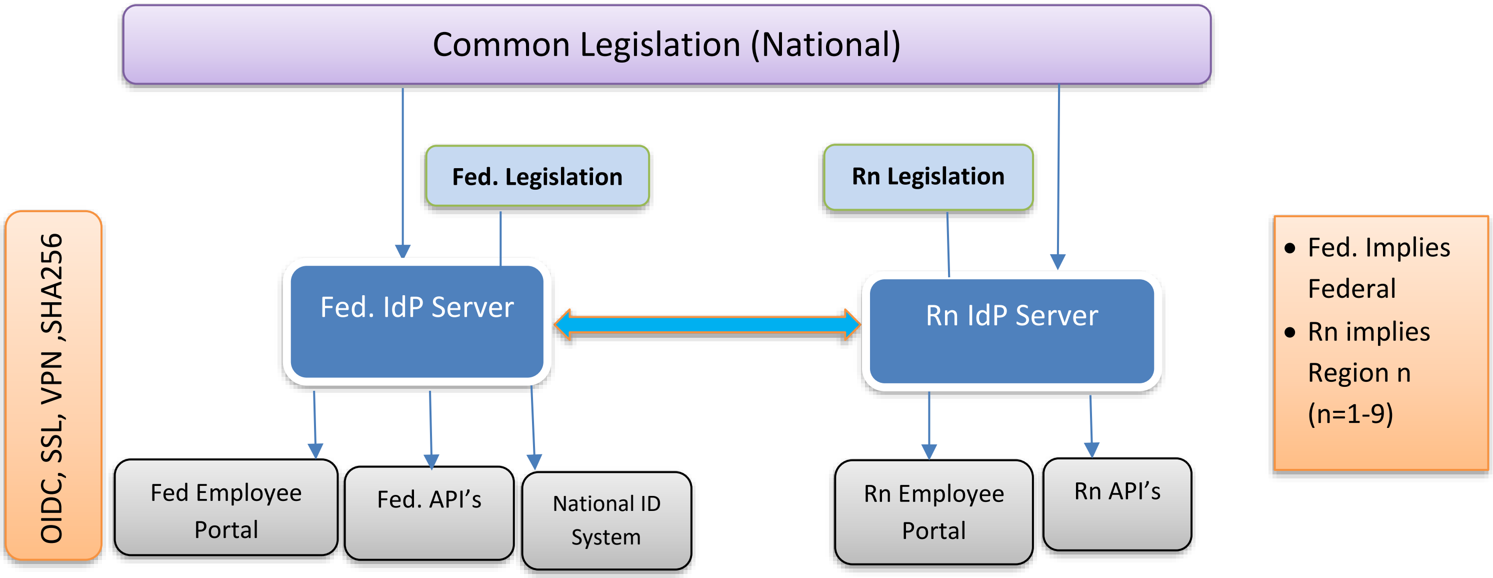


Figure 5. IDM Implementation Architectural Framework for Ethiopian E-Government

Common Legislation: vertical legal acts and standards between the federal government and regional governments, i.e. data protection, privacy and security, interoperability, administration, trust, and information sharing must be agreed to integrate and share effectively.

Federal & regional Legislations: these legislations and standards are used for horizontal communication between ministries at the federal level and between agencies/bureaus at the regional level.

Federal Identity provider (IDP): used to authenticate and authorize relying party (Employee portal), service providers (APIs), and users at ministries. This also used to authenticate and authorize regional clients which wants to access a common National ID platform. Implementing identity providers independently at the federal and regional levels will improve administration flexibility, security, and privacy.

National ID: The national ID is used as a base platform for all systems to identify the identities of all the citizens in the country. This platform includes the vital events information of citizens and used as a back-end platform to provide services and share information across organizations.

Regional identity provider (Rn IDP): used to authenticate and authorize regional relying party (RP), APIs, and users. Regional IDPs implemented based on national and regional standards. These IDPs assures the privacy and security issues during vertical communications with other regional and federal systems.

Employee Portal: Employee portals or relying parties' are client-side web applications. Users at each level use employee portals to access distributed organizational resources through the identity provider (IDP).

APIs: Application programming interfaces (API) are found distributed at each organization. The fragmented systems data sharing and other services are provided using these APIs. The APIs are accessed through the identity providers by those relying parties which have fulfilled the regional or/and national authorization requirements.

OpenID Connect: is a federation communication protocol build on top of oAuth. OIDC used to authenticate and authorize the relying party (Employee portal), a service provider (API), and users during the communication through an identity provider (IDP).

SHA256: used to encrypt all the tokens during authentication and authorization communication between identity provider, relying party, and API endpoints. Encrypting all communications between entities ensures confidentiality.

SSL: used to sign all the communications between the IDP, RP, and SP to ensure integrity and non-repudiation.

VPN: To integrate and share data at back-office using the existing governmental Woreda-net private network improves the reliability of the communication between the entities.

3.4 Developing and Evaluating Artifact

Use case scenario

We have selected three organizations from the Amhara region namely trade bureau, revenue bureau, and vital events agency. All three organizations have inter-connected functionalities. Trade bureau main functionalities are trade license registration and yearly license renewal. One person can have multiple licenses inside the Amhara region or elsewhere in Ethiopia. The Amhara revenue bureau collects taxes from merchants which have a trade license at the regional bureau. Those merchants who want to renew their trade license must pay the previous year taxes expected from them. Regional vital events agency registers the death, birth, marriage, and divorce events of all the peoples of the region. To get the trade license registration, to identify the number of licenses inside or outside of the region, to view citizen’s tax payment profiles and citizens' basic profiles could be identified based on his/her nationally unique identification number. Only the necessary data of citizen’s share across organizations. Revenue bureau gives the privilege to view the merchant’s current tax payment profile, and the trade bureau gives the privilege to view all the trade license profiles of customers. We used regional vital events agencies 17 digit birth certificate number as citizen identification number since it is unique throughout the country.

Development Groundwork

The designed interoperable identity management framework would be used to implement federated identity management which can work horizontally and vertically among the regional and the federal governments. The main objective of this thesis would be the establishment of data sharing across fragmented systems in different government agencies, and the exchange of identity information in a secure and reliable channel.

The software used for the federated identity management implementation is Microsoft Asp.Net core 2.2 framework to implement employee’s portal and API resources. IdentityServer4, OpenID connect protocol and Identity server starter kit UI is used to implement the identity provider; Microsoft Visual Studio 2019 Community Edition was the integrated development environment within which all these applications were developed and tested; SQL Server 2017 Express edition is used as a database tool for resources and APIs data management. All the tools used to develop the IDM system and the resources are free to download and use.

3.4.1 Developing the Artifact

Phase one: The API resources of the selected organizations namely Trade API, Revenue API were built first, then the employee portal application was built to work for horizontal integration. The organizational data management handled at the API side using Microsoft SQL server 2017 edition. We used as a national ID, a seventeen digit birth certificate number that identifies citizen's location region, zone, Woreda, Kebele, birth year, and a three-digit number. All the locations in the country have a unique id. Currently at regional and national level citizens are identified based on the birth certificate Id number of the above criteria.

Phase two: The authorization policy, OIDC authentication, scopes, and resource secrets were set from both directions at the API side and the client application side. The authorization policy is based on the agreed data sharing requirements between government entities.

Phase three: The Identity server designed was flexible and simple to associate and disassociate all the API, client, and identity resources. The administrator of the identity server registered all APIs, Client, and Identity resources. The administrator also assigned the roles, scopes, and privileged resources for all registered users. The IDP stores, authenticate, and authorizes all the resources.

Phase four: In this phase, we made the exchange of identity information between relying parties and identity servers in a secure network. All the identity information sent from the identity provider to relying parties was signed with a self-signed certificate that was created and assigned to the identity provider. SHA256 was the digital signing algorithm used by the identity provider. All the communication between the relying party and the identity provider was using HTTP and SSL protocol for end-to-end encryption. Validation token attached with each response to avoid cross-site request forgery.

Phase five: in the fifth phase we implemented the single-sign-out functionality from both sides at the relying party and identity provider. The single-sign-out functionality enables the user to global logout from the identity provider and each of the logged-in relying parties. Authentication cookies and tokens are destroyed as soon as the user logged out.

Phase six: In this phase Ministries of the Federal government integrates horizontally using federal employee portal and federal IDP to access API resources distributed at their offices. Regional governments also have their Regional employee portal and IDP to access API resources at regional agencies or bureaus with reliable security and privacy. Each regional and federal government would have its data-sharing policies to be implemented in their administrative areas. Implementing IDP at each level of governance improves the privacy of citizens and governments since the authentication, authorization, administration, and data sharing policy handled by themselves.

Even though there are different design options to access multiple APIs distributed at each agency's server, we chose a method in which a user requests an access token for a single API through the web portal and stores the token at the browser cookies and reuses it for other API calls. Whenever the user wants to access another API the client doesn't request another access token instead it reuses the previously stored access token at the cookie and sent the request to the resource server. This method minimizes the communication between the client application and the identity provider to get access token for each resource.

Phase Seven: To achieve vertical and inter-regional integration, we used one common employee portal and one common IDP. The common IDP authenticates all the privileged users from all the regions and national governments to access regional and national resources. The national data sharing or authorization policy would be implemented at the common portal and each regional APIs that are registered at Common IDP for vertical integration.

Figure 6. The Communication between User, Employee Portal (RP) and IDP

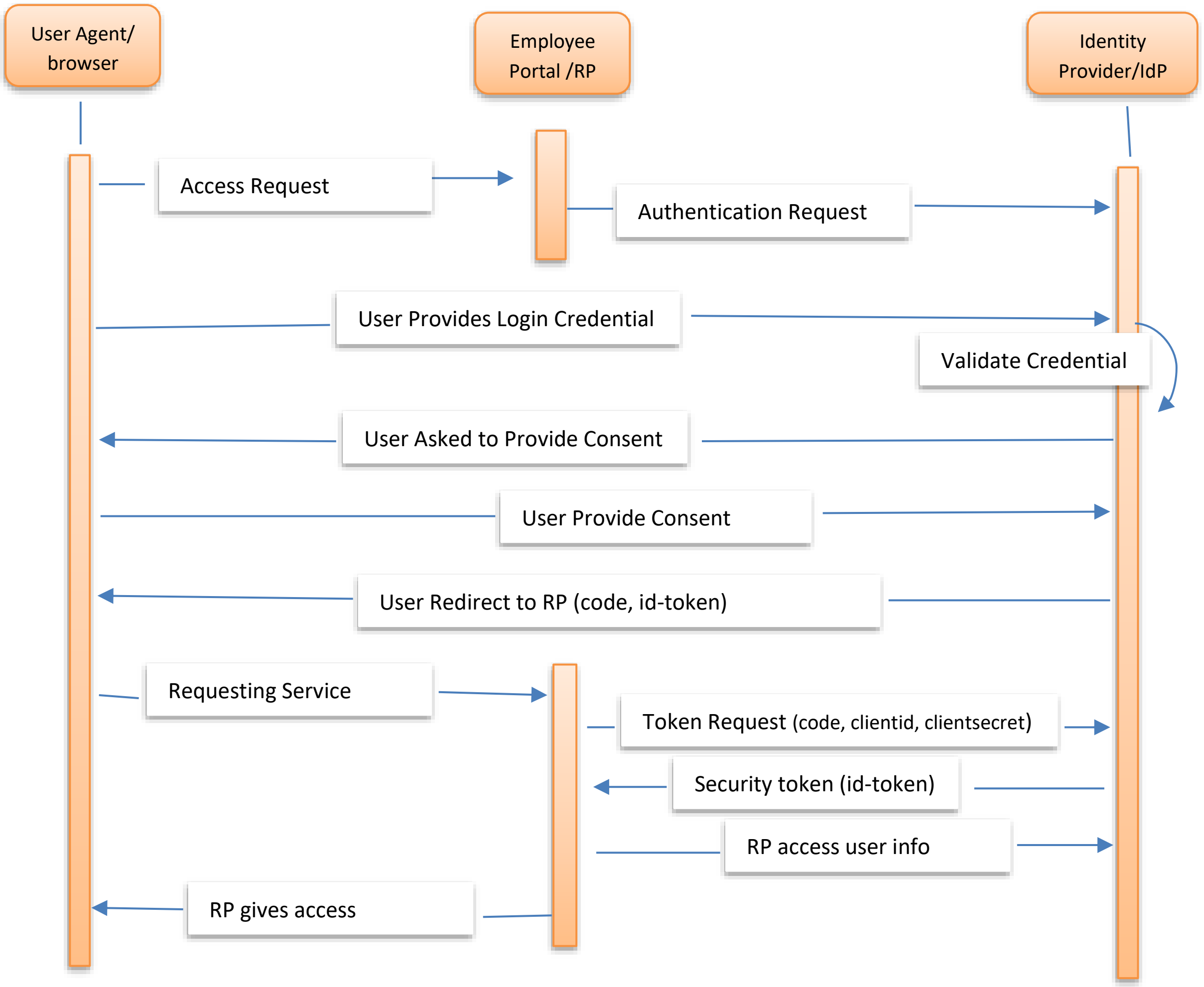


Figure 7. Communication Flow diagram to access single organization resource.

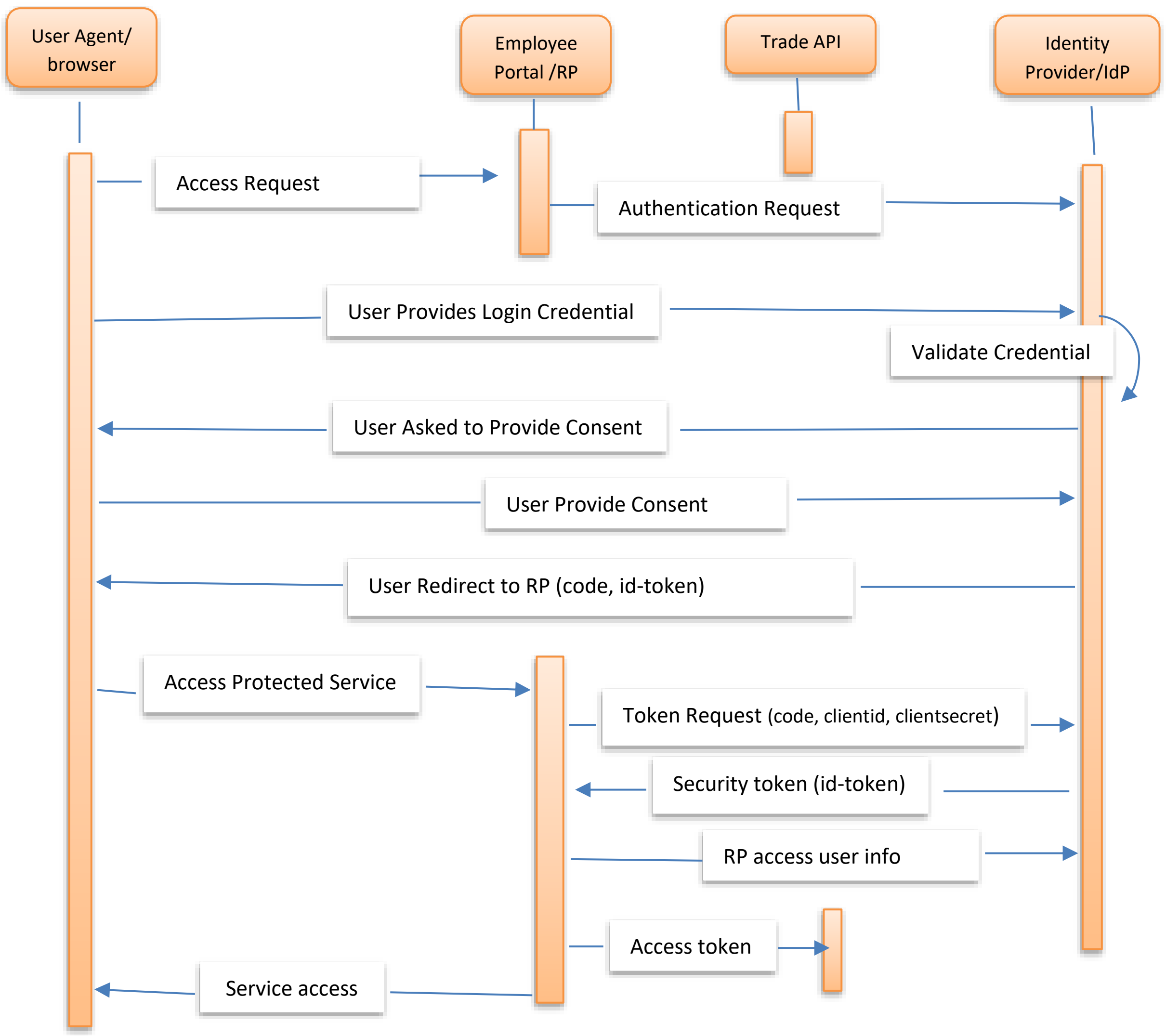
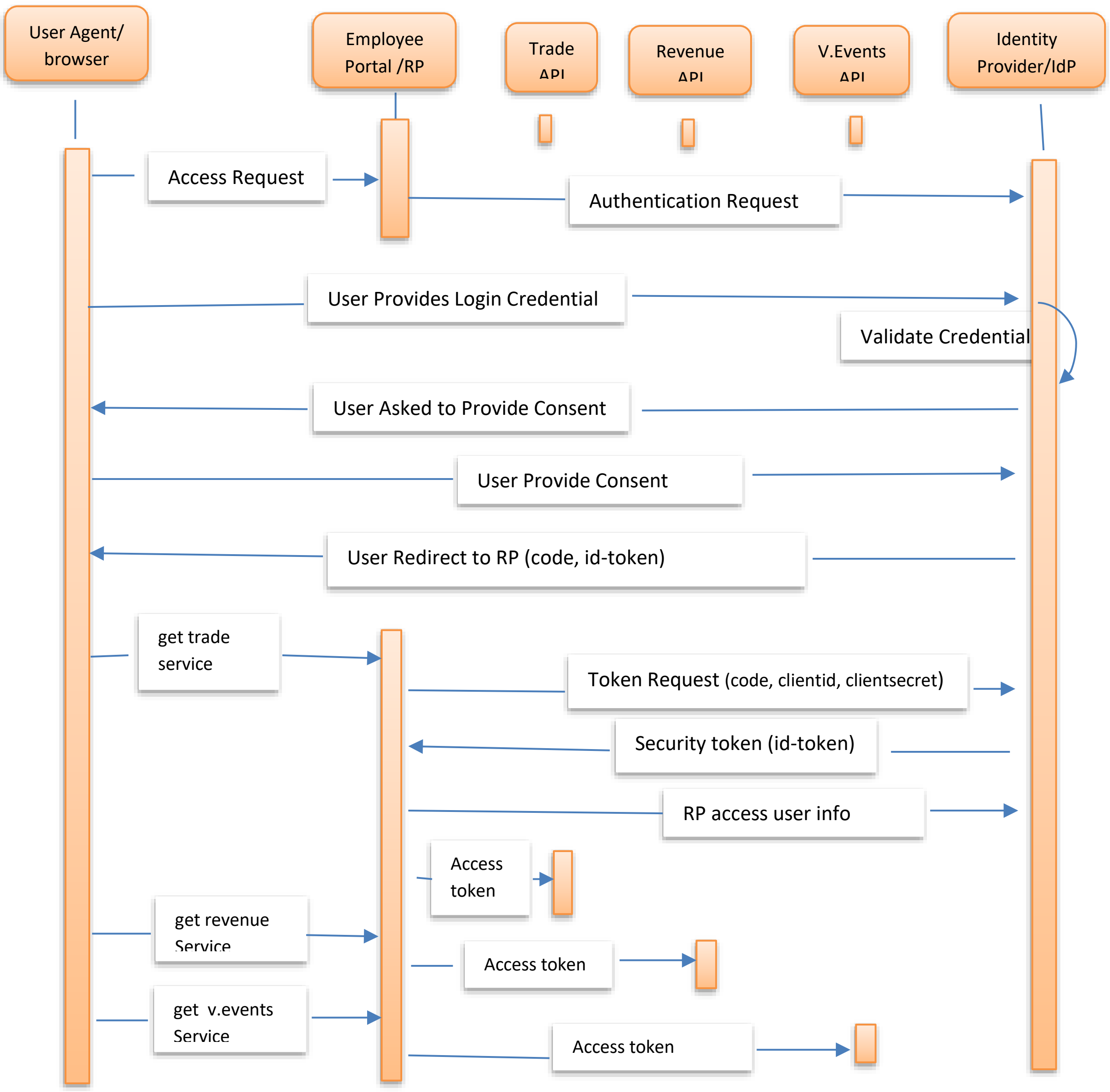


Figure 8. Communication diagram flow to access multiple organization services



Analysis of the Artifact Development

The developed artifact has included all the selected technical requirements of identity management implementation based on the designed government architecture focusing on integrating fragmented government systems for better public service delivery. The identity model requirements are covered in phase three. The privacy and security requirements are included in phase 2, phase 4, and phase5. The interoperability requirements are implicitly enabled by OIDC protocol and covered in phase 6 and phase 7.

The mapping between the development phases and requirements

No	Requirement Type	Phase
1	Identity Model	3
2	Privacy and security	2,4,5
3	Interoperability	6,7
4	Legislation(Authorization Policy)	2

3.4.2 Evaluating the framework

The designed artifact is an implementation framework that guides the process of real implementation of identity management for government ministries and agencies. The evaluation, therefore, requires measuring the quality of the framework. The quality attributes which are most suitable to analyze this framework are usability, interoperability, security, and completeness.

Usability: measures the extent to which the framework is practically usable in real scenarios by the government entities. To measure usability of the framework we chose two parameters, the first one is, the extent to which fragmented government systems can access and share distributed resources across the selected organizations in the use case scenario, and the second parameter is the extent to which the developed artifact is easily scalable and expandable to implement for multiple fragmented systems across ministries and agencies.

Technical Interoperability: measures the extent to which IDM and fragmented systems across organizations have remote access to databases or applications, share data, and use of similar open communication standards[80][31].

Security: Measures the extent to which the designed artifact is not vulnerable to DoS, XSS, and MIMA security threats of OIDC protocol. OIDC protocol is vulnerable to DoS attack during the use of publicly open and non-secure endpoints, XSS attack when the attacker exploits recent sessions for previously authorization granted client, MIMA attacks during the dynamic registration of clients**.** The proposed solutions for those security threats are using secured API endpoints, refreshing tokens for every new request, and handling the client registration only from the identity provider side**.** The security evaluation process has measured the extent to which all three solutions are included or not.

Completeness: measures the extent to which the framework meets the broad set of requirements determined in the requirement phase[81].

The type of specific artifact leads to the choice of an evaluation method. Based on the study on design science evaluation methods [82], using one or more experts to evaluate IT frameworks is a more suitable and most widely used method of evaluation. We used two experts for face-to-face evaluation to assess the developed artifact[82].

From the selected two evaluators, one of the experts evaluated the framework from the end-user perspective while the other expert evaluated from the technical perspective. A feedback form was prepared to enable the evaluators to give their feedback in a structured format. The feedback form had one row each for the three quality attributes. Each row had a column to rate the framework on the corresponding quality criteria/parameters on the scale of 1 to 5 (5- Excellent, 4-Very Good, 3-Good, 2-Average, and 1-Poor) with 5 being the best score. There was an adjacent column to write comments or suggestions from the evaluator. The average of quality parameters took as a grade for each respective measurement attributes.

There were a few potential evaluators who were easily accessible during the research. These potential evaluators were contacted through phone. Two of the most experienced IT professionals who showed a willingness to participate in the research work were chosen as evaluators. The potential evaluators were selected based on their practical experience with software project evaluation and implementation and overall experience in the IT domain. We couldn't find a face-to-face evaluator who has technical experience in identity management implementation. The technical evaluator who has a master's degree in computer science and participated in different governmental software quality evaluation tasks. The second evaluator has a BSC degree and 8 years' experience in different IT positions.

Evaluation Result

The technical evaluator gives the IDM framework excellent for 3 of the quality attributes (Usability, interoperability, and security). On usability, the evaluator commented that the framework is usable in real IDM implementation of Ethiopian e-government and scalable to include multiple relying parties and service providers. On interoperability, the evaluators have commented the fragmented systems have remote access to each other to share data using common communication standards. The evaluator also commented that the artifact should include other platforms to measure the heterogeneous nature of open standard communication protocols. On completeness (score 4), the evaluator commented that the framework includes the necessary attributes of IDM technologies and government entities. From the security perspective, the evaluators commented that the designed artifact fulfills all the three security requirements. The evaluator suggested adding more technical detail on the implementation of IDM to make more usable for intermediate level developers.

The user evaluator graded the IDM framework as excellent (score 5) on the quality attributes – Usability and interoperability. On usability, the evaluator commented that the framework is very useful for real government implementation and enterprise-level big institutions. The completeness and security attributes were graded as very- good (score 4) and the evaluator suggested that the framework could include additional biometric authentication parameters (fingerprint) to add further functionality like online service delivery for citizens and security requirements of the deployment area.

Evaluation Summary

Both of the evaluators have rated the framework highly (greater than 4) for all the 4 attributes. They gave us very useful suggestions and comments for further improvement and inclusiveness. The first important suggestions are adding additional scopes like fingerprint authentication to minimize the digital divide for the extended future of citizen service delivery. The second important suggestion was to go deeper into the technical details of the development that could be inclusive of different levels of developer skills. Both of these suggestions were included in future work.

3.5 Discussion and Conclusion

The final explanations on the result, research contribution, limitations, and future works of this research work presented in this chapter.

3.5.1 Results

This thesis has demonstrated that government systems and services distributed across ministries and agencies can be connected and work together easily and effectively while maintaining confidentiality, privacy, and security. Major technical requirements for the establishment of identity management and interoperability have been identified and discussed. A major output of this research work is an interoperable identity management framework guides the way to integrate and share data from fragmented systems across government ministries and agencies for better public service delivery.

3.5.2 Research Contribution

Government service delivery and interoperability do not function well in many countries yet. Ensuring that an integrated approach is effective and sustained across ministries and agencies remains challenging[5][8]. The designed framework proposes an initial design that would assist decision-makers how suitably integrate ministries and agencies for better public service delivery using an interoperable IdM system. The framework also guides, how can integrate distributed systems with the necessary privacy and security requirements of customers and organizational data in particular.

As OIDC is a recent protocol, there are no enough papers done that guide the implementation of identity management in a distributed environment. This research also used as a foundation for software developers and researchers on the real implementation of identity management services in a distributed environment, relying party integration, and authorization policy issues.

3.5.3 Limitations

This thesis has the following limitations:-

- The study does not include biometric (fingerprint, iris, or facial recognition) identities.
- The study focused only on technical interoperability. Social and cultural aspects of electronic identity management have not been discussed in the thesis.
- The framework has not tested in a real implementation or production environment.

3.5.4 Conclusion

The overall main points and results of the research have presented in this chapter. Designing an interoperable identity management framework for government organizations focusing on integrating and sharing data across ministries and agencies was the main research objective wanted to meet.

Most of the existing governmental IDM frameworks designed in different countries (i.e. Australia and India) are aiming for efficient public electronic service (eService) delivery, which is the final stage of e-government. The integrated government uses as a backend platform for the implementation of eService delivery. Implementing IDM for eService delivery purposes requires different organizational, technical, privacy, and security requirements to collaborate with government organizations, private companies, and citizens[83][36][21]. But, this thesis focuses on integrating horizontally and vertically fragmented government systems by considering the scalability and expandability for future eService delivery implementation. All the actors in connected government systems are government employees and organizations.

The previously implemented and designed IDM frameworks are focusing at the national level, which does not consider the trust and flexibility of administrations for federated countries like Ethiopia, in which regional governments have autonomous power. The proposed framework enables us to adopt all the necessary legislation both at the national and regional levels.

This framework can be used as a foundation for those who wanted to implement government back integration and public service delivery. This framework can be extended by adding biometric authentication methods like iris and fingerprint to improve security as well as minimize the digital divide for the effective use of citizen public service delivery.

3.5.5 Future Work

Including additional biometric authentication methods like a fingerprint or/and iris improves the security of service delivery and minimizes identity theft. It also minimizes the digital divide especially in developing countries in which most of the people are illiterate. To provide government services for the whole of citizen biometric or token-based card authentication is mandatory. Therefore, the framework can be enhanced by adding these aspects to future work.

Social and cultural aspects have a significant effect on digital identity management implementation especially when we use it for citizen service delivery. Therefore, the framework can be broadened in scope to include these issues.

Implementing the federated identity management for horizontal and vertical integration needs detailed authorization policy or access control for all levels. Studying and implementing vertical and horizontal authorization requirements in real production can be another future work.

References

[1] OECD, "The Role of Digital Identity Management in the Internet Economy: A PRIMER FOR POLICYMAKERS," *Policy,* no. 2008, pp. 1–20, 2009.

[2] R. Baldoni and S. Antonio, *Federated Identity Management Systems in e-Government : the Case of Italy*, vol. x, no. x. 2009.

[3] E. Birrell and F. B. Schneider, "Federated identity management systems: A privacy-based characterization," *IEEE Secure. Priv.*, vol. 11, no. 5, pp. 36–48, 2013.

[4] T. Role *et al.*, "A Blueprint for Digital Identity," no. August 2016.

[5] U. Nations, *E-GOVERNMENT SURVEY 2016*. 2016.

[6] P. Key, N. D. Set, N. Enterprise, and S. Bus, "Executive Summary of the E-Government Strategy," pp. 1–23, 2013.

[7] H. De Vries, V. Bekkers, and L. Tummers, "Innovation in the public sector: A systematic review and future research agenda," *Public Adm.*, vol. 94, no. 1, pp. 146–166, 2016.

[8] OECD, "The OECD Privacy Framework," *Organ. Econ. Co-Operation Dev.*, pp. 1–154, 2013.

[9] Y. Levy and T. J. Ellis, "A systems approach to conduct an effective literature review in support of information systems research," *Informing Sci.*, vol. 9, no. May 2014, pp. 181–211, 2006.

[10] J. Vom Brocke, A. Simons, B. Niehaves, K. Riemer, R. Plattfaut, and A. Cleven, "Reconstructing the giant: On the importance of rigour in documenting the literature search process," *17th Eur. Conf. Inf. Syst. ECIS 2009*, no. December 2013, 2009.

[11] A. I. Segovia, D. Álvaro, and M. Enríquez, "Digital Identity : the current state of affairs."

[12] S. Sector and O. F. Itu, "ITU-T X.1254 Entity authentication assurance framework," vol. 1254, 2012.

[13] ITU, *Digital Identity Road Map Guide*. .

[14] D. W. Chadwick, "Federated Identity Management," pp. 96–120, 2009.

[15] G. Ben Ayed, *Architecting User-Centric Privacy-as-a-Set-of-Services*. 2014.

[16] I. T. U. Kaleidoscope, "Global Convergence in Digital Identity and Attribute Management : EMERGING NEEDS FOR Global Convergence in Digital Identity and Attribute Management : EMERGING NEEDS FOR," 2014.

[17] P. Beynon–Davies, "Personal identity management and electronic government: The case of the national identity card in the UK," *J. Enterp. Inf. Manag.*, vol. 20, no. 3, pp. 244–270, 2007.

[18] A. Rasiwasia, "A Framework To Implement OpenID Connect Protocol For Federated Identity Management In Enterprises," 2017.

[19] J. Kwame, "Aalborg Universitet A Case for Implementation of Citizen-Centric National Identity Management Systems Crafting a Trusted National Identity Management Policy A Case for Implementation of Citizen-Centric National Identity Management Systems : Crafting a Tru," 2013.

[20] H. L. Amrani, "Identity Management Systems : Techno - Semantic Interoperability for Heterogeneous Federated Systems," no. 3, pp. 102–111, 2018.

[21] C. Alemayehu and J. Mwangi, "An Interoperable Identity Management Solution for Kenya E-Government," *Pure.Ltu.Se,* 2012.

[22] J. Jensen, “Federated Identity Management and Usage Control - Obstacles to Industry Adoption,” pp. 31–41, 2013.

[23] J. Jensen, *Federated Identity Management in the Norwegian Oil and Gas Industry*, no. March. 2014.

[24] ID4D, “ID4D,” 2016.

[25] Danish National ID Centre, "The sub-regional administration - Sub cities The district administration - Approximately 800 Woredas The local administration - Approximately 15000 Kebeles 1," pp. 1–7, 2018.

[26] B. T. Negussie, “CITIZEN IDENTIFICATION SYSTEM: THE CASE FOR ETHIOPIA,” *Computer (Long. Beach. Calif).*, no. March 2007.

[27] Es. Portal, “Ethiopian eService portal,” 2019. .

[28] Es. Portal, “privacy policy,” 2019.

[29] M. Belachew, “E-Government Initiatives in Ethiopia,” no. May, 2014.

[30] K. D. Institute, *Strategy for the Implementation of e-Government*. 2013.

[31] Y. Ducq and D. Chen, “How to measure interoperability: Concept and approach,” *2008 IEEE Int. Technol. Manag. Conf. ICE 2008*, no. November, 2016.

[32] Z. Fang, “e-Goverment in digital era : concept, practice and development,” *Int. J. Comput. internet Manag.*, vol. 10, no. 2, pp. 1–22, 2002.

[33] S. Agrawal, S. Banerjee, and S. Sharma, “Privacy and Security of Aadhaar : A Computer Science Perspective,” pp. 1–23.

[34] ID4D, “Privacy by Design : Current Practices in Estonia , India , and Austria,” 2018.

[35] I. MCIT, “Interoperability Framework for e-Governance,” no. October, pp. 1–54, 2015.

[36] A. D. T. Agency, “Overview and Glossary,” no. March, 2019.

[37] Australian Digital Transformation Agency, “Attribute Profile,” no. March, 2019.

[38] D. Recordon and D. Reed, “OpenID 2.0: A platform for user-centric identity management,” *Proc. Second ACM Work. Digit. Identity Manag. DIM 2006. Co-located with 13th ACM Conf. Comput. Commun. Secur. CCS’06*, pp. 11–16, 2006.

[39] S. T. Sun, E. Pospisil, I. Muslukhov, N. Dindar, K. Hawkey, and K. Beznosov, “What makes users refuse web single sign-on?: An empirical investigation of OpenID,” *SOUPS 2011 - Proc. 7th Symp. Usable Priv. Secur.*, 2011.

[40] “SAML Tutorial: How SAML Authentication Works - SAML 2.0 SSO Flow Diagram.” [Online]. Available: https://developers.onelogin.com/saml. [Accessed: 13-Feb-2020].

[41] N. Naik, P. Jenkins, and D. Newell, “Choice of suitable Identity and Access Management standards for mobile computing and communication,” *Proc. 24th Int. Conf. Telecommun. Intell. Every Form, ICT 2017*, 2017.

[42] W. A. Alrodhan and A. I. Alqarni, “Security Investigation and Analysis of OpenID : Problems and Enhancements,” vol. 17, no. 10, pp. 198–211, 2017.

[43] B. Laurie, A. Langley, and E. Kasper, “RFC 6962: Certificate Transparency,” *RFC*, pp. 1–27, 2013.

[44] S. Engineering and A. Kivinen, “OpenID Connect Provider Certification,” 2019.

[45] B. B. Ki, “OPENID WITH CERTIFICATE-BASED USER AUTHENTICATION ON SMARTCARD By,” 2013.

[46] J. Mitchell, Wanpeng Li and Chris and Mitchell, “Analysing the Security of Google’s implementation of OpenID Connect Wanpeng,” no. July, pp. 25–34, 2016.

[47] OpenID Foundation, “OpenID Connect FAQ and Q&amp;As | OpenID.” [Online]. Available: https://openid.net/connect/faq/. [Accessed: 13-Feb-2020].

[48] OpenID Foundation, “OpenID Connect | OpenID.” [Online]. Available: https://openid.net/connect/. [Accessed: 13-Feb-2020].

[49] V. Mladenov, C. Mainka, and J. Schwenk, “On the security of modern Single Sign-On Protocols: Second-Order Vulnerabilities in OpenID Connect,” 2015.

[50] D. Fett, R. Küsters, and G. Schmitz, “A comprehensive formal security analysis of OAuth 2.0,” *Proc. ACM Conf. Comput. Commun. Secur.*, vol. 24-28-Octo, pp. 1204–1215, 2016.

[51] T. Groß, “Security analysis of the SAML single sign-on browser/artifact profile,” *Proc. - Annu. Comput. Secur. Appl. Conf. ACSAC*, vol. 2003-Janua, no. Acsac, pp. 298–307, 2003.

[52] S. Name and A. Sid, “Interoperability frameworks : analysis , comparison , and guidelines Interoperability frameworks : analysis , comparison , and guidelines,” no. December, 2017.

[53] A. Armando, R. Carbone, L. Compagna, J. Cuellar, G. Pellegrino, and A. Sorniotti, “From multiple credentials to browser-based single sign-on: Are we more secure?,” *IFIP Adv. Inf. Commun. Technol.*, vol. 354 AICT, no. 216471, pp. 68–79, 2011.

[54] J. H. P. M. P. M. Nick Ragouzis, “(SAML) V2.0 Technical Overview.” [Online]. Available: http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html. [Accessed: 16-Feb-2020].

[55] N. Naik, P. Jenkins, P. Davies, and D. Newell, “Native web communication protocols and their effects on the performance of web services and systems,” *Proc. - 2016 16th IEEE Int. Conf. Comput. Inf. Technol. CIT 2016, 2016 6th Int. Symp. Cloud Serv. Comput. IEEE SC2 2016 2016 Int. Symp. Secur. Priv. Soc. Netwo*, pp. 219–225, 2017.

[56] A. Abuarqoub, “A lightweight two-factor authentication scheme for mobile cloud computing,” *ACM Int. Conf. Proceeding Ser.*, no. September 2014, 2019.

[57] N. Naik, “Migrating from Virtualization to Dockerization in the Cloud: Simulation and Evaluation of Distributed Systems,” *Proc. - 2016 IEEE 10th Int. Symp. Maint. Evol. Serv. Cloud-Based Environ. MESOCA 2016*, pp. 1–8, 2016.

[58] oAuth0, “JSON Web Token Introduction - jwt.io.” [Online]. Available: https://jwt.io/introduction/. [Accessed: 01-Mar-2020].

[59] S. C. Sukumaran and M. Mohammed, “PCR and Bio-signature for data confidentiality and integrity in mobile cloud computing,” *J. King Saud Univ. - Comput. Inf. Sci.*, no. July, 2018.

[60] W3.org, “XML Security � Issues and Requirements.” [Online]. Available: https://www.w3.org/2007/xmlsec/ws/papers/09-lockhart-bea/. [Accessed: 01-Mar-2020].

[61] N. Samaan and A. Karmouch, “Towards autonomic network management: An analysis of current and future research directions,” *IEEE Commun. Surv. Tutorials*, vol. 11, no. 3, pp. 4–21, 2009.

[62] oAuth0, “Critical vulnerabilities in JSON Web Token libraries.” [Online]. Available: https://auth0.com/blog/critical-vulnerabilities-in-json-web-token-libraries/. [Accessed: 01-Mar-2020].

[63] N. Heijmink, “Secure Single Sign-On,” 2015.

[64] S.-T. Sun, “Towards Improving the Usability and Security of Web Single Sign-On Systems,” 2013.

[65] D. Kreutz, E. Feitosa, H. Cunha, H. Niedermayer, and H. Kinkelin, “Increasing the resilience and trustworthiness of OpenID identity providers for future networks and services,” *Proc. - 9th Int. Conf. Availability, Reliab. Secur. ARES 2014*, no. Section III, pp. 317–324, 2014.

[66] R. Hörbe, “Privacy by Design in Federated Identity Management,” pp. 167–174, 2015.

[67] “Final: OpenID Authentication 2.0 - Final.” [Online]. Available: https://openid.net/specs/openid-authentication-2_0.html. [Accessed: 01-Mar-2020].

[68] A. Van der Merwe, A. Gerber, and H. Smuts, “Guidelines for Conducting Design Science Research in Information Systems,” pp. 1–16, 2016.

[69] M. A. R. Ken Peffers, Tuure Tuunanen, “A Design Science Research Methodology for Information Systems Research,” *J. Manag. Inf. Syst.*, vol. 73, no. 48, pp. 4201–04, 2007.

[70] M. Denscombe, *O pen UP Study Skills The Good Research Guide*. .

[71] K. Cameron, “The Laws of Identity | Microsoft Docs,” 2007. [Online]. Available: https://docs.microsoft.com/en-us/previous-versions/dotnet/articles/ms996456(v=msdn.10)?redirectedfrom=MSDN. [Accessed: 15-Jun-2020].

[72] R. Hörbe, “Privacy by Design in Federated Identity Management,” no. July 2015, 2018.

[73] World Bank Group, “ID4D-Practitioner-s-Guide.”

[74] J. H. Hoepman, *Making Privacy by Design Concrete*, vol. abs/1501.0, no. December. 2018.

[75] Australian Digital Transformation Agency, “Technical Requirements,” no. March, 2019.

[76] World Bank Group, “Technical Standards for Digital Identification Systems,” 2018.

[77] Wikipedia, “Aadhaar - Wikipedia,” 2016. [Online]. Available: https://en.wikipedia.org/wiki/Aadhaar#Lack_of_legislation_and_privacy_concerns. [Accessed: 19-Feb-2020].

[78] Republic of Estonia, “Estonian eID scheme : ID card,” 2018.

[79] G. Merugu, “Requirements elicitation and access: A research,” *Int. J. Innov. Technol. Explor. Eng.*, vol. 8, no. 11 Special Issue, pp. 903–905, 2019.

[80] G. da Silva Serapião Leal, W. Guédria, and H. Panetto, “Interoperability assessment: A systematic literature review,” *Comput. Ind.*, vol. 106, pp. 111–132, 2019.

[81] J. Venable, J. Pries-Heje, and R. Baskerville, “FEDS: A Framework for Evaluation in Design Science Research,” *Eur. J. Inf. Syst.*, vol. 25, no. 1, pp. 77–89, 2016.

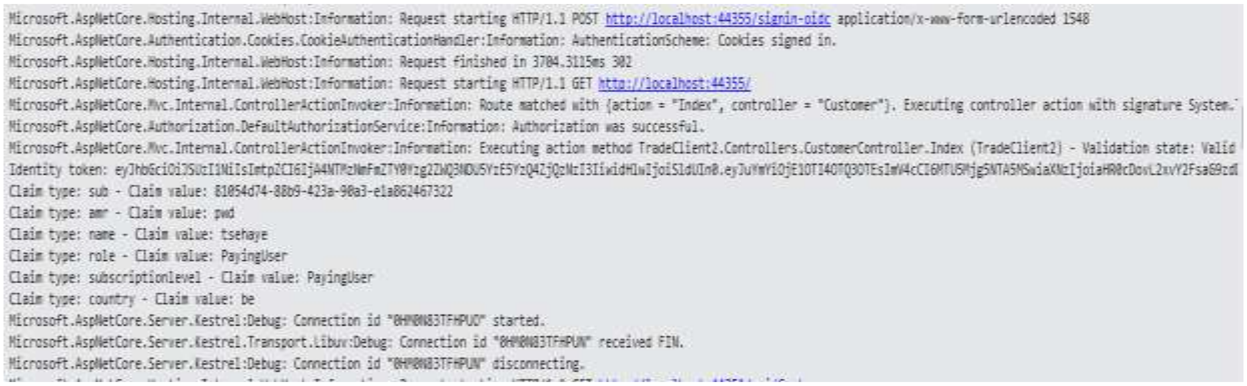
[82] K. Peffers, M. Rothenberger, T. Tuunanen, and R. Vaezi, “Design Science Research Evaluation,” pp. 398–410, 2012.

[83] I. T. U. Publications, *Digital identity in the ICT ecosystem: An overview*. 2018.

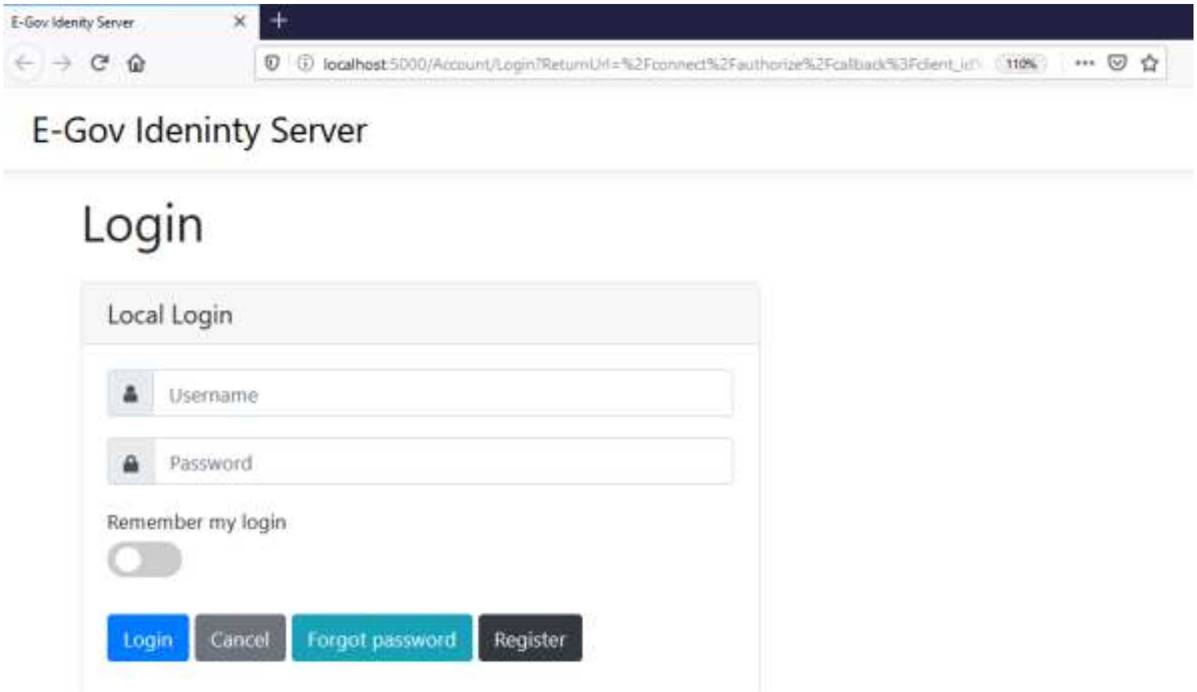
Appendices

1 Login Page

A user requesting to access the employee portal redirects to identity provider server for authentication and authorization. First, the identity provider authenticates employee portal (relying party) by its client ID and secret key. Then, the identity provider requests the user to enter its credentials and redirect to the employee portal.



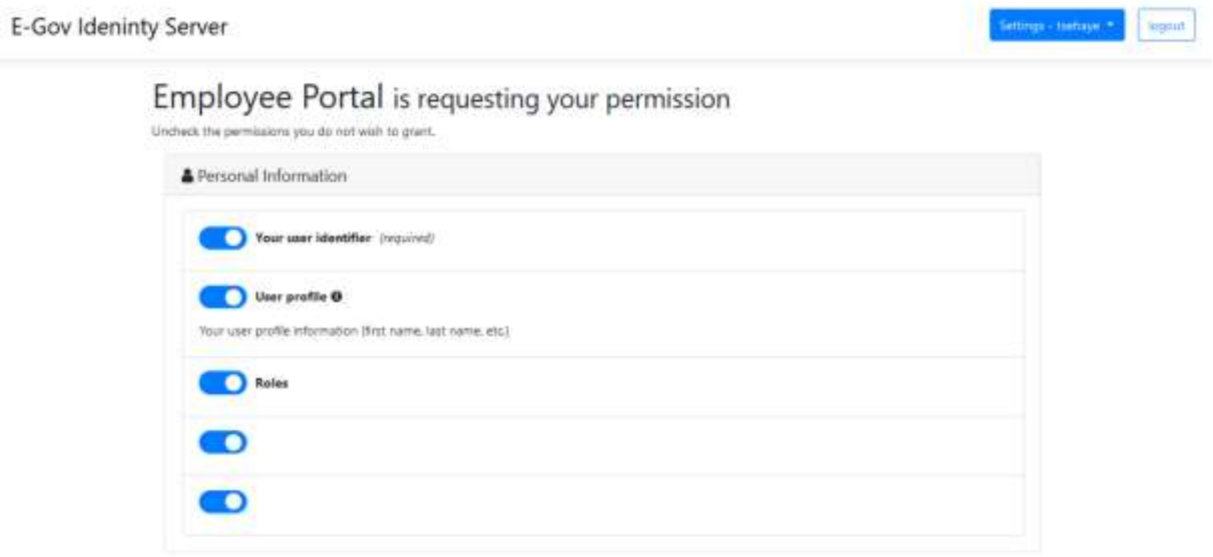
```
Microsoft.AspNetCore.Hosting.Internal.WebHost:Information: Request starting HTTP/1.1 POST http://localhost:44355/signin-oidc application/x-www-form-urlencoded 1548
Microsoft.AspNetCore.Authentication.Cookies.CookieAuthenticationHandler:Information: AuthenticationScheme: Cookies signed in.
Microsoft.AspNetCore.Hosting.Internal.WebHost:Information: Request finished in 3704.3115ms 302
Microsoft.AspNetCore.Hosting.Internal.WebHost:Information: Request starting HTTP/1.1 GET http://localhost:44355/
Microsoft.AspNetCore.Mvc.Internal.ControllerActionInvoker:Information: Route matched with {action = "Index", controller = "Customer"}. Executing controller action with signature System.
Microsoft.AspNetCore.Authorization.DefaultAuthorizationService:Information: Authorization was successful.
Microsoft.AspNetCore.Mvc.Internal.ControllerActionInvoker:Information: Executing action method TradeClient2.Controllers.CustomerController.Index (TradeClient2) - Validation state: Valid
Identity token: eyJhbGciOiJSUzI1NiIsImtpZCI6IjA4NTMzNmFmZTY0Yzg2ZWQ3NDU5YzE5YzQ4ZjQzMzI3IiwidHlwIjoiSldUIn0.eyJuYmYiOjE1OTI4OTQ3OTEsImV4cCI6MTU5Mjg5NTA5MSwiaXNzIjoiaHR0cDovL2xvY2FsaG9zdH
Claim type: sub - Claim value: 81054d74-88b9-423a-90a3-e1a862467322
Claim type: amr - Claim value: pwd
Claim type: name - Claim value: tsehaye
Claim type: role - Claim value: PayingUser
Claim type: subscriptionlevel - Claim value: PayingUser
Claim type: country - Claim value: be
Microsoft.AspNetCore.Server.Kestrel:Debug: Connection id "0HM0N83TFHPUO" started.
Microsoft.AspNetCore.Server.Kestrel.Transport.Libuv:Debug: Connection id "0HM0N83TFHPUN" received FIN.
Microsoft.AspNetCore.Server.Kestrel:Debug: Connection id "0HM0N83TFHPUN" disconnecting.
```



9.2 Consent Screen

After the user enters his/her password/username credentials the identity provider requests the user to allow or not the employee portal to access your profile. And shows the list of API resources allowed to use. This part assures one of the user privacy principles of identity management systems.

User profile consent



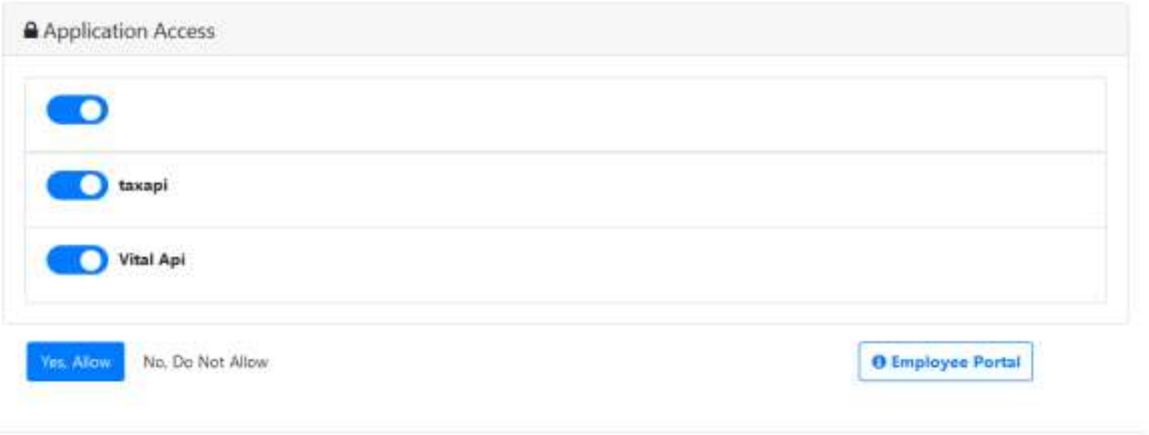
Employee Portal is requesting your permission

Uncheck the permissions you do not wish to grant.

Personal Information

- ● Your user identifier (required)
- ● User profile
  Your user profile information (first name, last name, etc)
- ● Roles
- ●
- ●

Application Consent

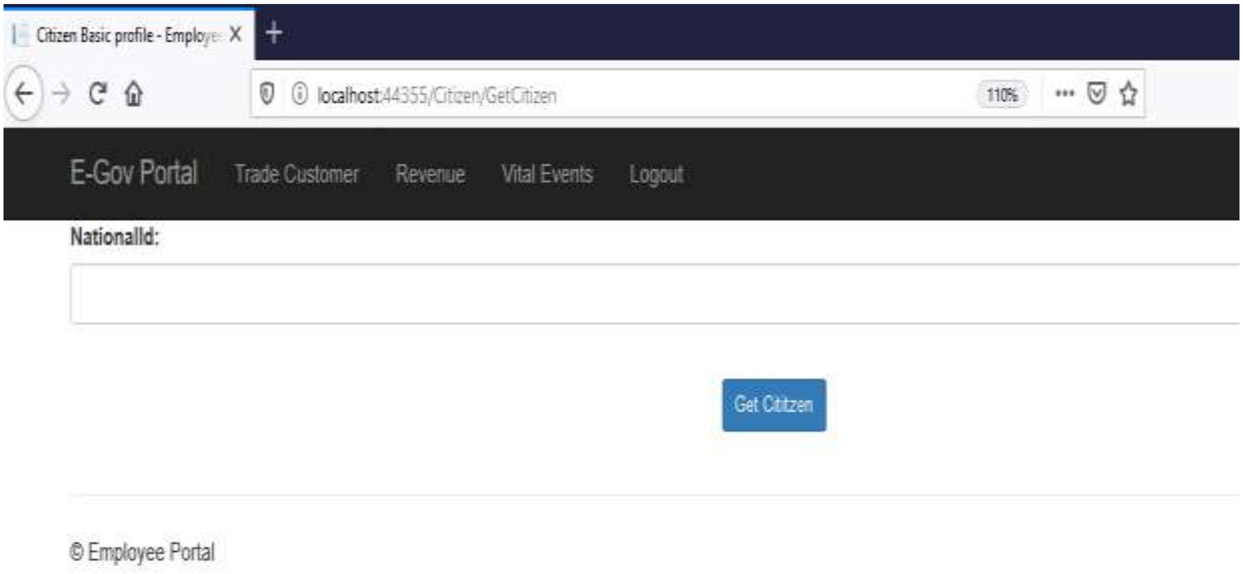


Application Access

- ●
- ● taxapi
- ● Vital Api

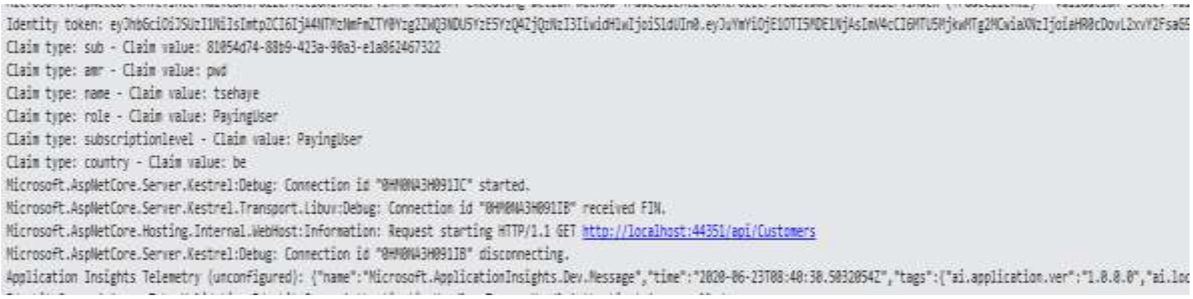
2 Employee portal

After successful completion of user authentication, the identity server redirects the user to employee portal. Then, Employee portal requests the identity provider the profiles of the logged-in user. This portal delivers all the services based on the logged-in user privilege.



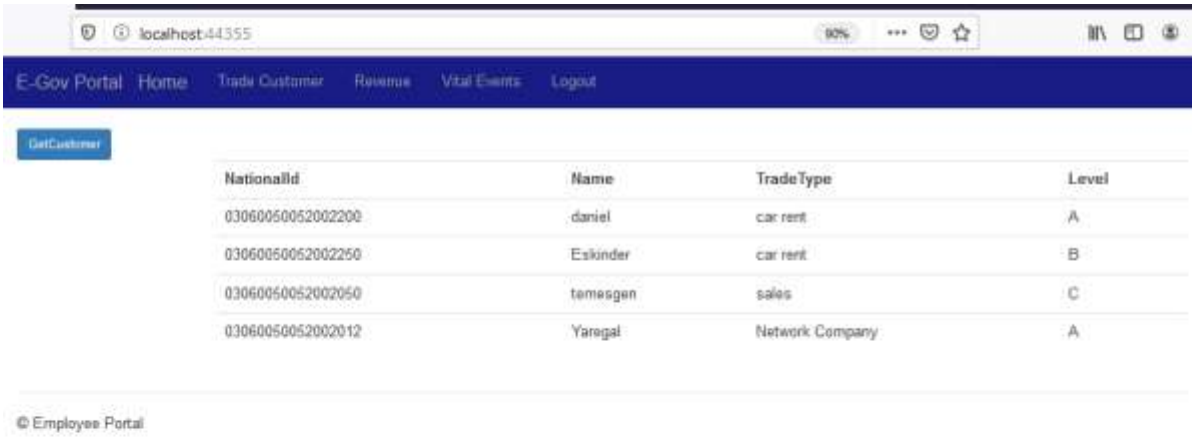
3 Accessing the first Organizational resource (Trade API)

The employee portal calls the first API based on the user information provided by the identity provider. All the user profiles and access tokens are sent to the employee portal during the API requests.



```
Identity token: eyJhbGciOiJSUzI1NiIsImtpZCI6IjA4NTMzNmFmZTY0Yzg2ZWQ3NDU5YzE5YzQ4ZjQzNzI3IiwidHlwIjoiSldUIn0.eyJuYmYiOjE1OTI5MDE1NjAsImV4cCI6MTU5MjkwMTg2MCwiaXNzIjoiaHR0cDovL2xvY2FsaG
Claim type: sub - Claim value: 81054d74-88b9-423a-90a3-e1a862467322
Claim type: amr - Claim value: pwd
Claim type: name - Claim value: tsehaye
Claim type: role - Claim value: PayingUser
Claim type: subscriptionlevel - Claim value: PayingUser
Claim type: country - Claim value: be
Microsoft.AspNetCore.Server.Kestrel:Debug: Connection id "0HM0NA3H091IC" started.
Microsoft.AspNetCore.Server.Kestrel.Transport.Libuv:Debug: Connection id "0HM0NA3H091IB" received FIN.
Microsoft.AspNetCore.Hosting.Internal.WebHost:Information: Request starting HTTP/1.1 GET http://localhost:44351/api/Customers
Microsoft.AspNetCore.Server.Kestrel:Debug: Connection id "0HM0NA3H091IB" disconnecting.
Application Insights Telemetry (unconfigured): {"name":"Microsoft.ApplicationInsights.Dev.Message","time":"2020-06-23T08:40:30.5032054Z","tags":{"ai.application.ver":"1.0.0.0","ai.loc
```

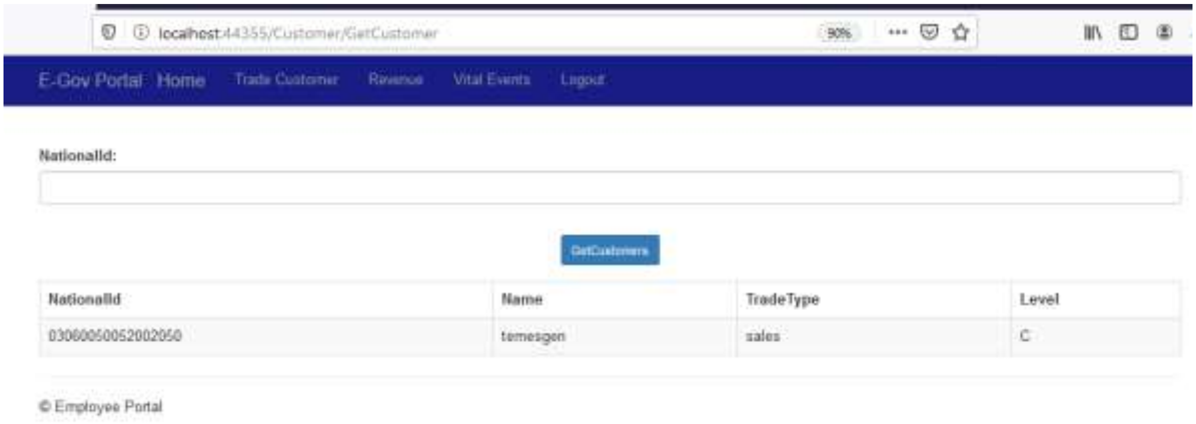
List of Trade customers



NationalId	Name	TradeType	Level
03060050052002200	daniel	car rent	A
03060050052002250	Eskinder	car rent	B
03060050052002050	temesgen	sales	C
03060050052002012	Yaregal	Network Company	A

© Employee Portal

Finding trade Customer using customers National ID



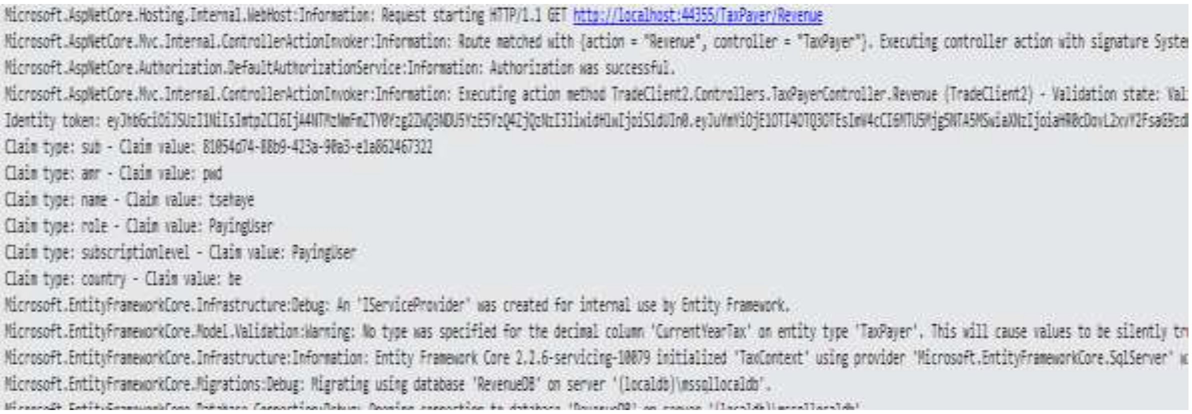
NationalId:

NationalId	Name	TradeType	Level
03060050052002050	temesgen	sales	C

© Employee Portal

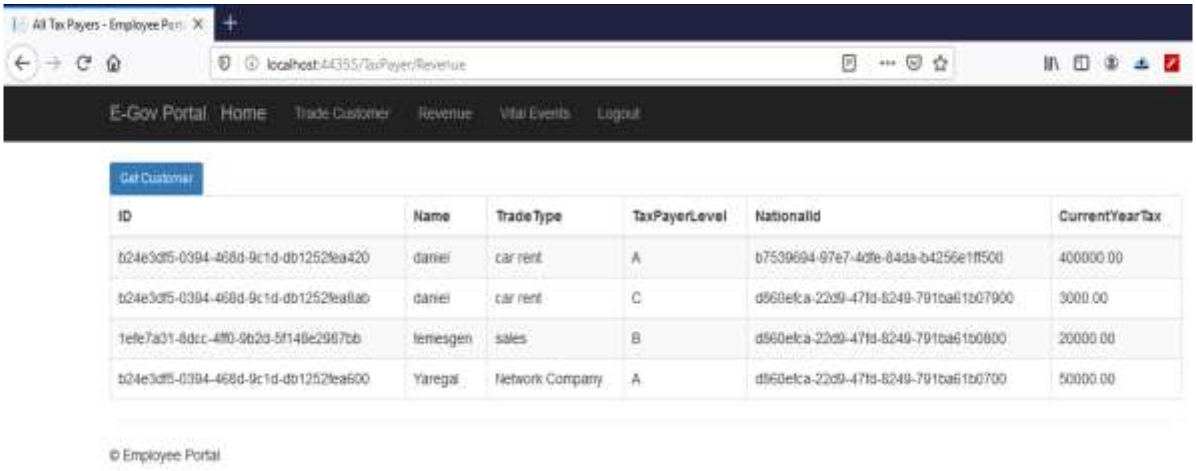
4 Accessing Revenue Bureau resources (API)

To access the second API, the employee's portal uses the same access token which previously got from the identity provider.



```
Microsoft.AspNetCore.Hosting.Internal.WebHost:Information: Request starting HTTP/1.1 GET http://localhost:44355/TaxPayer/Revenue
Microsoft.AspNetCore.Mvc.Internal.ControllerActionInvoker:Information: Route matched with {action = "Revenue", controller = "TaxPayer"}. Executing controller action with signature Syste
Microsoft.AspNetCore.Authorization.DefaultAuthorizationService:Information: Authorization was successful.
Microsoft.AspNetCore.Mvc.Internal.ControllerActionInvoker:Information: Executing action method TradeClient2.Controllers.TaxPayerController.Revenue (TradeClient2) - Validation state: Val
Identity token: eyJhbGciOiJSUzI1NiIsImtpZCI6IjA4NTMzMmFmZTY0YzgzZWQ3NDU5YzE5YzQ4ZjQzNzI3IiwidHlwIjoiSldUIn0.eyJuYmYiOjE1OTI4OTQ3OTEsImV4cCI6MTU5Mjg5NTA5MSwiaXNzIjoiaHR0cDovL2xvY2FsaG9zd
Claim type: sub - Claim value: 81054d74-88b9-423a-98a3-e1a862467322
Claim type: amr - Claim value: pwd
Claim type: name - Claim value: tsehaye
Claim type: role - Claim value: PayingUser
Claim type: subscriptionlevel - Claim value: PayingUser
Claim type: country - Claim value: be
Microsoft.EntityFrameworkCore.Infrastructure:Debug: An 'IServiceProvider' was created for internal use by Entity Framework.
Microsoft.EntityFrameworkCore.Model.Validation:Warning: No type was specified for the decimal column 'CurrentYearTax' on entity type 'TaxPayer'. This will cause values to be silently tr
Microsoft.EntityFrameworkCore.Infrastructure:Information: Entity Framework Core 2.2.6-servicing-10079 initialized 'TaxContext' using provider 'Microsoft.EntityFrameworkCore.SqlServer' w
Microsoft.EntityFrameworkCore.Migrations:Debug: Migrating using database 'RevenueDB' on server '(localdb)\mssqllocaldb'.
Microsoft.EntityFrameworkCore.Database.Connection:Debug: Opening connection to database 'RevenueDB' on server '(localdb)\mssqllocaldb'.
```

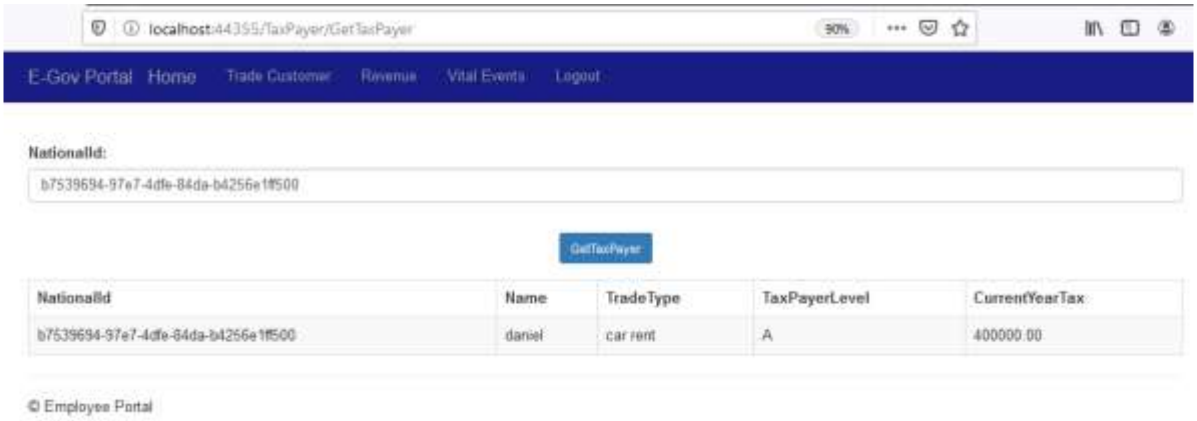
List of Taxpayers



ID	Name	TradeType	TaxPayerLevel	NationalId	CurrentYearTax
b24e3df5-0394-468d-9c1d-db1252fea420	daniel	car rent	A	b7539694-97e7-4dfe-84da-b4256e1ff500	400000.00
b24e3df5-0394-468d-9c1d-db1252fea8ab	daniel	car rent	C	d860efca-22d9-47fd-8249-791ba61b07900	3000.00
1efe7a31-8dcc-4ff0-9b2d-5f148e2987bb	temesgen	sales	B	d860efca-22d9-47fd-8249-791ba61b0800	20000.00
b24e3df5-0394-468d-9c1d-db1252fea600	Yaregal	Network Company	A	d860efca-22d9-47fd-8249-791ba61b0700	50000.00

© Employee Portal

Searching Tax Payers

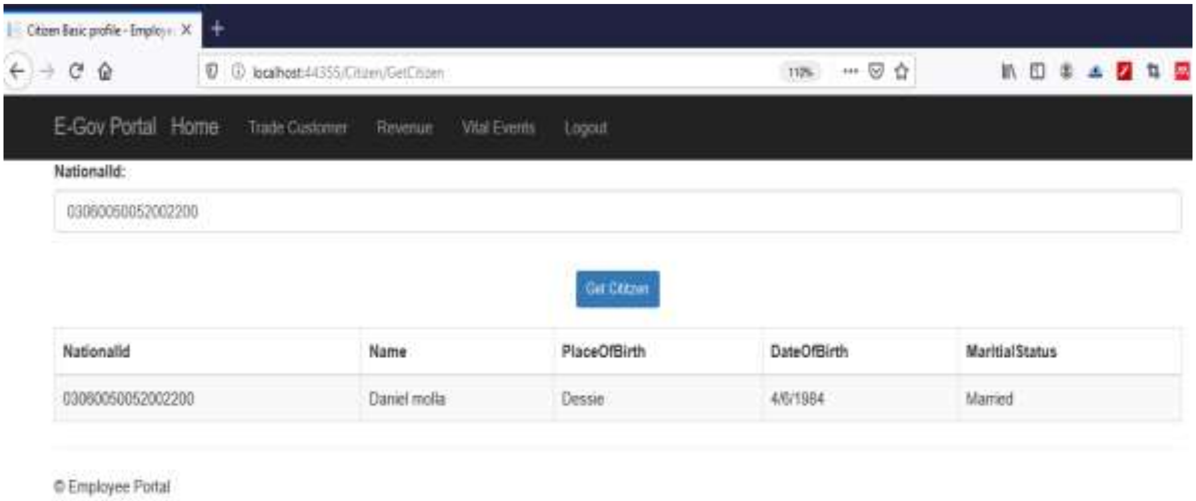


NationalId: b7539694-97e7-4dfe-84da-b4256e1ff500

NationalId	Name	TradeType	TaxPayerLevel	CurrentYearTax
b7539694-97e7-4dfe-84da-b4256e1ff500	daniel	car rent	A	400000.00

© Employee Portal

5 Finding Citizen from national API



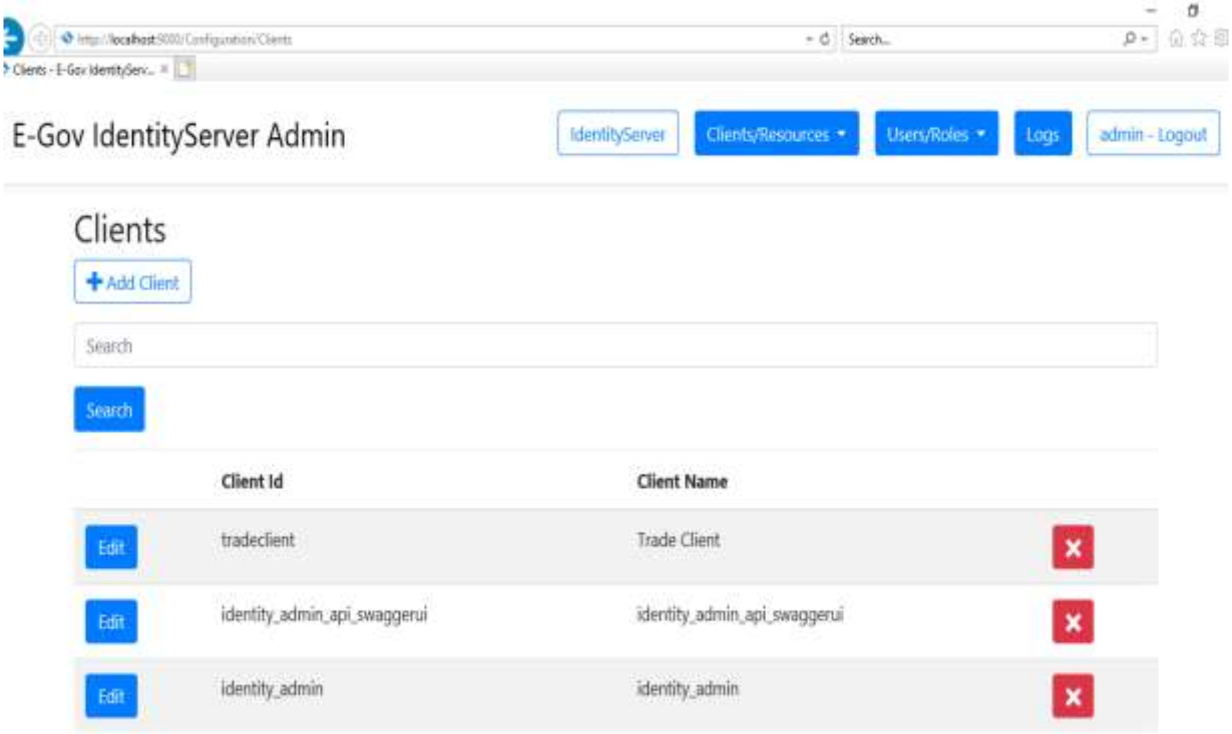
NationalId:

03060050052002200

NationalId	Name	PlaceOfBirth	DateOfBirth	MaritialStatus
03060050052002200	Daniel molla	Dessie	4/6/1984	Married

© Employee Portal

6 Relying party registration page

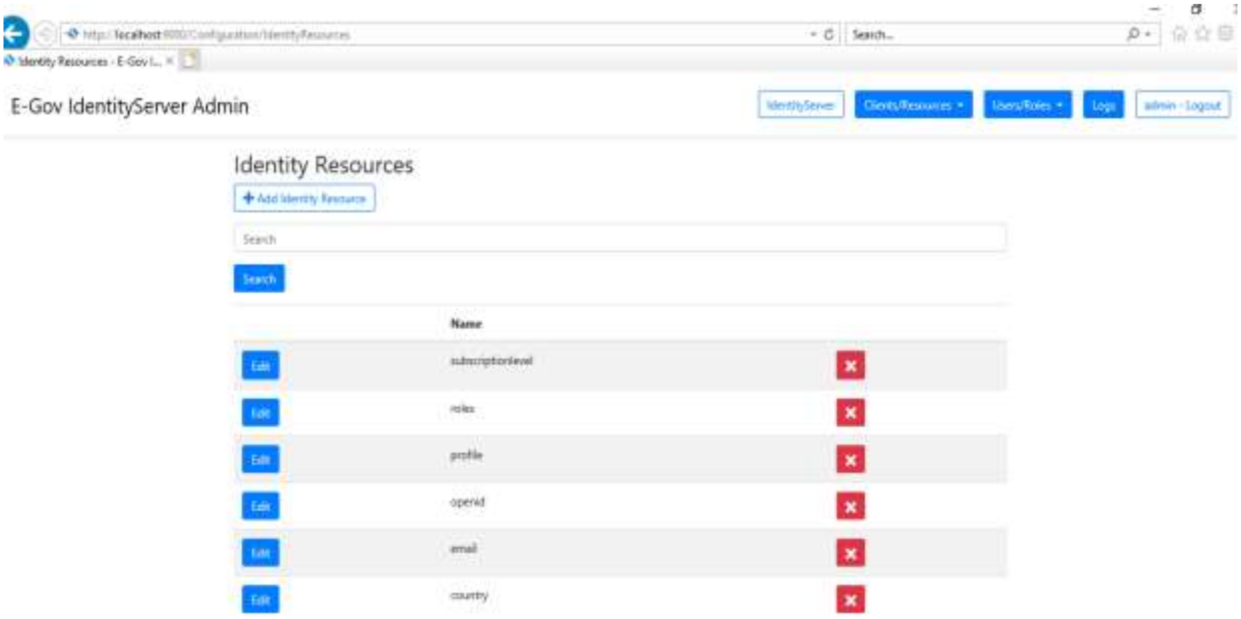


E-Gov IdentityServer Admin

Clients

	Client Id	Client Name	
Edit	tradeclient	Trade Client	✕
Edit	identity_admin_api_swaggerui	identity_admin_api_swaggerui	✕
Edit	identity_admin	identity_admin	✕

7 Identity resources

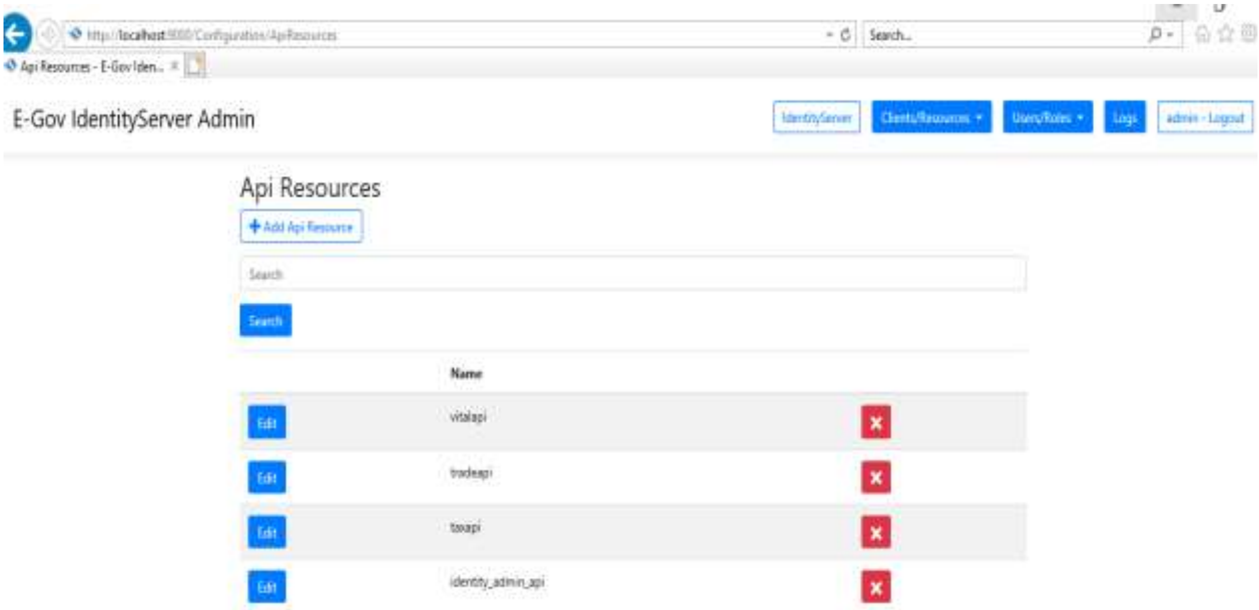


E-Gov IdentityServer Admin

Identity Resources

	Name	
Edit	subscriptionlevel	✕
Edit	roles	✕
Edit	profile	✕
Edit	openid	✕
Edit	email	✕
Edit	country	✕

8 API resources

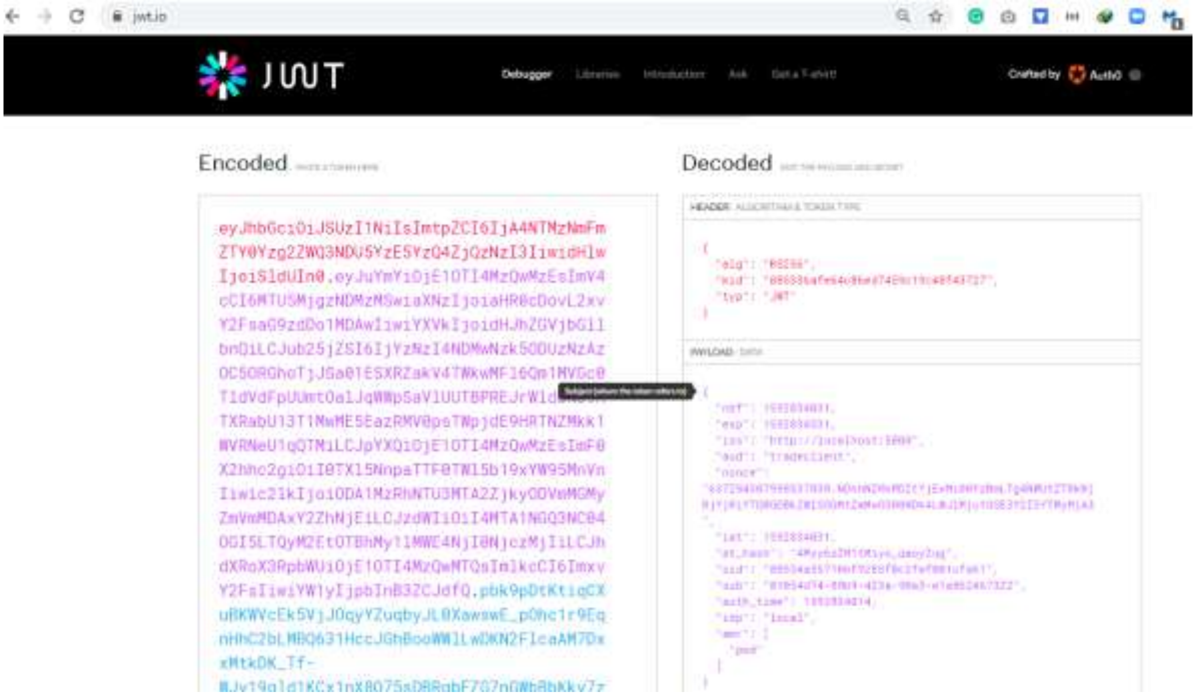


E-Gov IdentityServer Admin

Api Resources

	Name	
Edit	vitalapi	✕
Edit	tradeapi	✕
Edit	taxapi	✕
Edit	identity_admin_api	✕

9 Decoded access token using jwt site

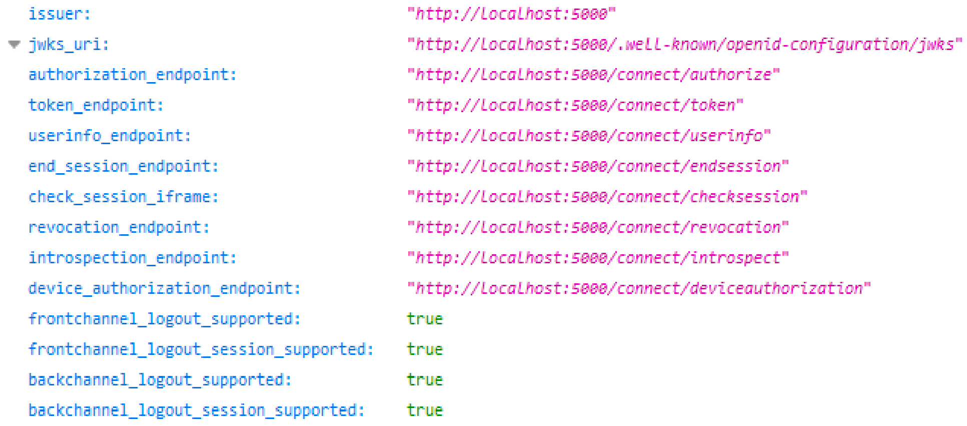


```
eyJhbGciOiJSUzI1NiIsImtpZCI6IjA4NTMzNmFm
ZTY0Yzg2ZWQ3NDU5YzE5YzQ4ZjQzNzI3IiwidHlw
IjoiSldUIn0.eyJuYmYiOjE1OTI4MzQwMzEsImV4
cCI6MTU5MjgzNDMzMSwiaXNzIjoiaHR0cDovL2xv
Y2FsaG9zdDo1MDAwIiwiYXVkIjoidHJhZGVjbGll
bnQiLCJub25jZSI6IjYzNzI4NDMwNzk5ODUzNzAz
OC5ORGhoTjJGa01ESXRZakV4TWkwMF16Qm1MVGc0
T1dVdFpUUmt0alJqWWp5aV1UUTBPREJrW1d
TXRabU13T1MwME5EazRMV0psTWpjdE9HRTNZMkk1
WVRNeU1qQTMiLCJpYXQiOjE1OTI4MzQwMzEsImF0
X2hhc2giOiI0TX15NnpaTTF0TW15b19xYW95MnVn
Iiwic2lkIjoiODA1MzRhNTU3MTA2ZjkyODVmMGMy
ZmVmMDAxY2ZhNjE1LCJzdWIiOiI4MTA1NGQ3NC04
OGI5LTQyM2EtOTBhMy11MWE4NjI0NjczMjIiLCJh
dXRoX3RpbWUiOjE1OTI4MzQwMTQsImlkcCI6Imxv
Y2FsIiwiYW1yIjpbInB3ZCJdfQ.pbk9pDtKtiqCX
uBKWVcEk5VjJ0qyYZuqbyJL0XawswE_p0hc1r9Eq
nHhC2bLMBQ631HccJGhBooWWlLwDKN2FlcaAM7Dx
xMtkDK_Tf-
WJv19q1d1KCx1nX8O75sD8RqbF7G7nGWb8bKkv7z
```

```
{
  "alg": "RS256",
  "kid": "[illegible]",
  "typ": "JWT"
}
```

```
{
  "nbf": [illegible],
  "exp": [illegible],
  "iss": "http://localhost:5000",
  "aud": "tradeclient",
  "nonce":
"[illegible]",
  "iat": [illegible],
  "at_hash": "[illegible]",
  "sid": "[illegible]",
  "sub": "[illegible]",
  "auth_time": [illegible],
  "idp": "local",
  "amr": [
    "pwd"
  ]
}
```

10 Discovery document configurations



```
  issuer:                              "http://localhost:5000"
▼ jwks_uri:                            "http://localhost:5000/.well-known/openid-configuration/jwks"
  authorization_endpoint:              "http://localhost:5000/connect/authorize"
  token_endpoint:                      "http://localhost:5000/connect/token"
  userinfo_endpoint:                   "http://localhost:5000/connect/userinfo"
  end_session_endpoint:                "http://localhost:5000/connect/endsession"
  check_session_iframe:                "http://localhost:5000/connect/checksession"
  revocation_endpoint:                 "http://localhost:5000/connect/revocation"
  introspection_endpoint:              "http://localhost:5000/connect/introspect"
  device_authorization_endpoint:       "http://localhost:5000/connect/deviceauthorization"
  frontchannel_logout_supported:       true
  frontchannel_logout_session_supported: true
  backchannel_logout_supported:        true
  backchannel_logout_session_supported: true
```