КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ІМЕНІ ТАРАСА ШЕВЧЕНКА

ФАКУЛЬТЕТ РАДІОФІЗИКИ, ЕЛЕКТРОНІКИ ТА КОМП'ЮТЕРНИХ СИСТЕМ

Кафедра радіотехніки та радіоелектронних систем

До захисту допущено: «На правах рукопису»
Завідувач кафедри _____ Ігор АНІСІМОВ
« __ » червня 2023 р.

КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА

на тему:

«СИСТЕМИ ДЕЛЕГОВАНОЇ АВТЕНТИФІКАЦІЇ»

Виконав:
студентка 4-го курсу
денної форми навчання
спеціальності 172 - Телекомунікації та радіотехніка
ОП «Інформаційна безпека телекомунікаційних систем і мереж»
Куліненко Вікторія Миколаївна _____

Науковий керівник:
к.ф.-м.н., ас. Котов Михайло Миколайович _____

Рецензент:
к.ф.-м.н., доц. Загороднюк Сергій Петрович _____

Засвідчую, що у цій бакалаврській роботі
немає запозичень з праць інших авторів без
відповідних посилань
Студент _____

Робота допущена до захисту в ЕК рішенням кафедри радіотехніки та радіоелектронних систем від «22» червня 2023 р., протокол № 21.

Завідувач кафедри радіотехніки та радіоелектронних систем,
доктор фіз.-мат. наук, професор
Анісімов Ігор Олексійович _____

Київ – 2023

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

OAuth – Open Authorization, протокол авторизації, який дозволяє користувачам надавати обмежений доступ до своїх ресурсів аплікаціям та сервісам без необхідності розкривати свої облікові дані.

SAML – Security Assertion Markup Language (мова розмітки декларації безпеки). Використовується для обміну даними про автентифікацію та авторизацію між сторонами.

XML – Extensible Markup Language (розширювана мова розмітки). Використовується для представлення та обміну структурованих даних у текстовому форматі.

API – Application Programming Interface інтерфейс програмування застосунків), набір правил та протоколів, що дозволяють різним програмам та сервісам взаємодіяти між собою.

JWT – JSON Web Tokenвідкритий стандарт для структуризованої передачі інформації у форматі JSON (JavaScript Object Notation).

SSL/TLS – Secure Sockets Layer/Transport Layer Security, протоколи шифрування та забезпечення безпеки, що використовуються для захисту передачі даних через мережу.

ВСТУП

Завдяки стрімкому розвитку технологій, все більше людей користуються онлайн-сервісами, такими як соціальні мережі, електронна комерція, банківські та фінансові послуги, хмарні зберігання даних та багато інших. Однак, це також призводить до зростання ризиків в сфері кібербезпеки, таких як крадіжка особистих даних, шахрайство та несанкціонований доступ до акаунтів. Традиційні методи автентифікації, зокрема використання паролів, часто виявляються недостатньо надійними та вразливими перед атаками зловмисників. Це пояснюється тим, що багато користувачів використовують слабкі паролі, повторюють їх на різних платформах або падають жертвами фішингових атак. Такі проблеми ставлять під загрозу безпеку та конфіденційність особистих даних користувачів. У цьому контексті системи делегованої автентифікації набувають великої актуальності. Вони дозволяють користувачам автентифікуватися на різних платформах та сервісах, використовуючи один обліковий запис, який вже мають у популярних сервісах, наприклад Google, Facebook або Twitter. Це спрощує процес автентифікації для користувачів, а також допомагає уникнути проблем, пов'язаних з керуванням багатьма паролями. Крім того, системи делегованої автентифікації пропонують покращену безпеку, оскільки вони використовують сучасні протоколи шифрування та механізми безпеки для передачі даних про автентифікацію. Вони також дозволяють користувачам зберігати контроль над своїми персональними даними та обмежувати обсяг інформації, яку надають стороннім сервісам.

У сучасному цифровому світі, де безпека та захист особистих даних є критичними факторами, розуміння принципів та застосування систем делегованої автентифікації стає все більш важливим. Дослідження в цій галузі може допомогти у розробці нових технологій та рекомендацій, що допоможуть поліпшити безпеку та зручність процесу автентифікації для користувачів та організацій.

Мета дослідження:

Метою моєї дипломної роботи є дослідження систем делегованої автентифікації з метою з'ясування їх принципів, переваг та недоліків, а також вивчення конкретних систем, що застосовуються у різних сферах. Головною метою є визначення ефективності та придатності цих систем для забезпечення безпеки та зручності процесу автентифікації користувачів у різних сервісах.

РОЗДІЛ 1.АВТЕНТИФІКАЦІЯ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

1.1 Основні поняття та принципи автентифікації

Автентифікація є ключовим поняттям в області інформаційної безпеки та захисту даних. У цьому розділі наведено детальний огляд основних понять, пов'язаних з автентифікацією, що дозволяє краще розуміти процес автентифікації, різних методів та принципів, що лежать в основі технології. Це також допоможе в подальшому визначити переваги та недоліки різних підходів до автентифікації та їх застосовність у різних сценаріях використання.[1]

1. Ідентифікація: Це перший крок в автентифікаційному процесі і відноситься до визначення ідентичності користувача або суб'єкта, який намагається отримати доступ до системи чи ресурсу. Ідентифікація зазвичай здійснюється шляхом представлення унікального ідентифікатора, такого як ім'я користувача, електронна адреса або номер акаунта.
2. Підтвердження: Цей етап включає перевірку ідентичності особи, яка намагається отримати доступ. Підтвердження зазвичай вимагає представлення додаткових даних або факторів, які можуть підтвердити ідентичність користувача. Наприклад, це може бути пароль, біометричні дані (відбитки пальців, розпізнавання обличчя), фізичні об'єкти (смарт-карти, USB-токени) або одноразові коди.
3. Авторизація: Цей етап відбувається після успішної автентифікації і визначає, які права та привілеї має користувач після отримання доступу до системи. Авторизація контролює, до яких ресурсів чи функціональності користувач може мати доступ.
4. Фактори автентифікації: В автентифікаційному процесі можуть використовуватись різні фактори, які забезпечують підтвердження ідентичності користувача. Зазвичай їх поділяють за трьома категоріями: володіння, знання, властивості.
5. Протоколи автентифікації: У світі інформаційної безпеки існує безліч протоколів та стандартів, які використовуються для реалізації автентифікації. Наприклад, протоколи OAuth, OpenID Connect, SAML та інші. Кожен з них має свої особливості, переваги та використання за різних сценаріїв.

Принципи автентифікації, що визначають основні правила та підходи, які використовуються для забезпечення безпеки та підтвердження особи користувача, наведені у табл.1.1.

Табл.1.1 Основні принципи автентифікації

Принцип	Пояснення	Приклади
Впізнавання	Система може впізнати та ідентифікувати користувача.	Унікальний номер акаунту, електронна пошта
Знання	Користувач має таємне знання, що підтверджує його ідентичність.	Пароль, пін-код, відповідь на контрольне питання
Володіння	Користувач має фізичний об'єкт, що підтверджує його ідентичність.	Смарт-карта, USB-токен, мобільний пристрій
Властивості	Користувач має унікальні фізичні характеристики для ідентифікації.	Відбиток пальця, розпізнавання обличчя, голос
Час	Час використовується як фактор автентифікації.	Одноразові паролі, синхронізовані токени

1.2 Принципи та переваги делегованої автентифікації

Делегована автентифікація - це процес, в якому користувач може надати дозвіл третій стороні (наприклад, іншому сервісу або додатку) використовувати його ідентифікаційні дані для отримання доступу до ресурсу без необхідності надавати свої облікові дані. Цей принцип ґрунтується на ідеї, що користувач може автентифікуватися один раз на центральному сервері або провайдері ідентичності, і після цього використовувати ці автентифікаційні дані для доступу до різних послуг або ресурсів, які підтримують делеговану автентифікацію [2, 3].

Ключові аспекти принципів делегованої автентифікації наведені у табл.1.2.

Табл.1.2. Ключові аспекти делегованої автентифікації

Аспект	Пояснення
Передача довіри	Делегована автентифікація передає довіру від однієї системи до іншої, що дозволяє використовувати ідентичність користувача.
Централізоване керування	Існує централізована система керування ідентичністю, яка перевіряє та підтверджує ідентичність користувача.
Протоколи та стандарти	Використовуються протоколи (OAuth, OpenID Connect, SAML тощо) для обміну ідентифікаційною інформацією між системами.
Ролі та дозволи	Після автентифікації, система може передати користувачу відповідні ролі, привілеї та доступ до ресурсів згідно з політиками.
Захист конфіденційності	Важливо застосовувати шифрування та захист даних під час передачі ідентичності користувача.
Гнучкість та зручність	Делегована автентифікація забезпечує зручний доступ до ресурсів без необхідності повторного введення автентифікаційних даних.

Процес делегованої автентифікації передбачає, що один сервіс може автентифікувати користувача через інший сервіс, щоб надати доступ до своїх ресурсів без необхідності вводити додаткові дані аутентифікації. На Рис 1.1 зображено процес після ініціювання сервісу А процес делегованої автентифікації, запитуючи користувача про його згоду на надання доступу до своїх ресурсів сервісу В.

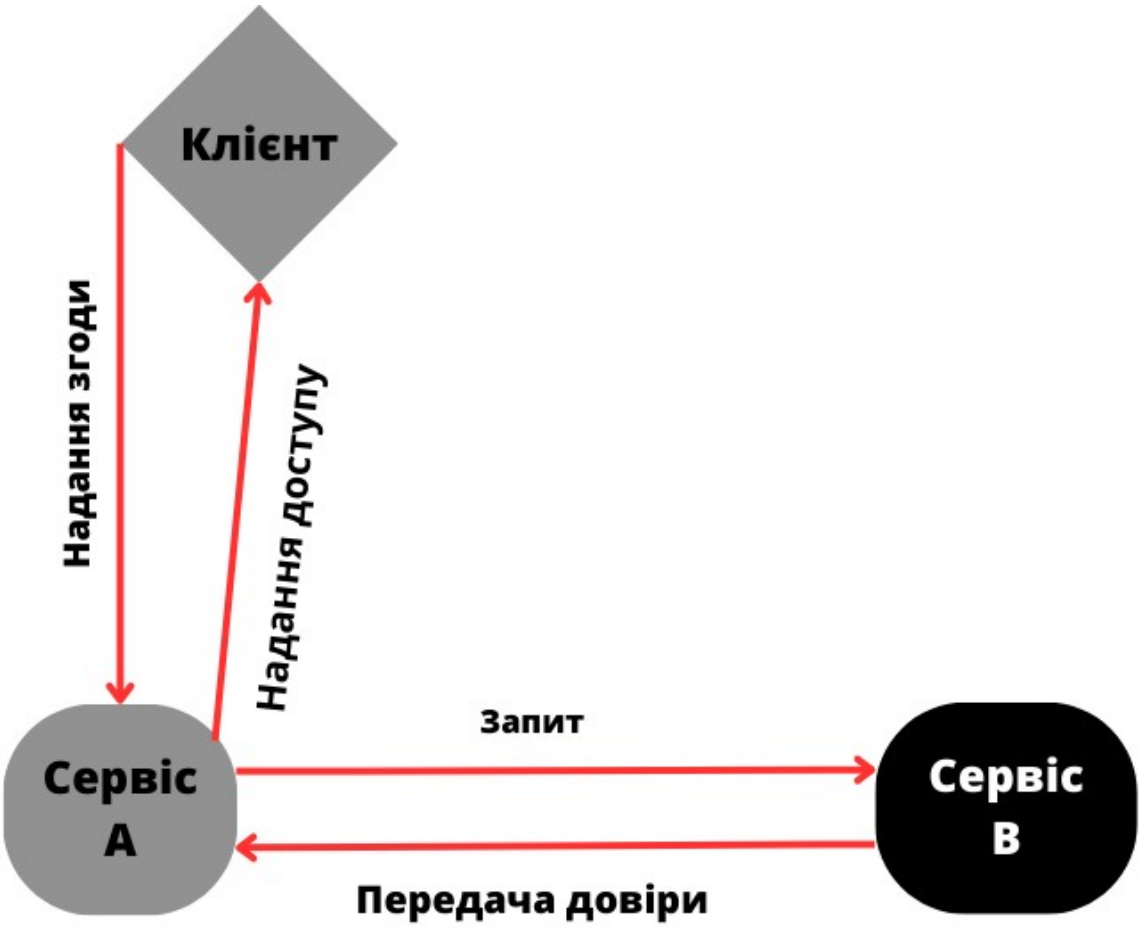

Рис.1.1 Процес делегованої автентифікації

Принципи делегованої автентифікації забезпечують використання інноваційного підходу до автентифікаційних процесів, що відкриває широкі можливості для зручного та безпечного доступу до різноманітних послуг та ресурсів. Подані принципи дозволяють впроваджувати ефективну делеговану автентифікацію, яка має ряд переваг [4]:

1) Зручність та спрощення процесу: Делегована автентифікація дозволяє користувачам уникнути необхідності запам'ятовувати та вводити багато різних облікових даних для доступу до різноманітних сервісів. Замість цього, після одноразової автентифікації на провайдері ідентичності, користувач може отримати доступ до багатьох сервісів без додаткового введення облікових даних.
2) Зменшення ризику витоку даних: Завдяки делегованій автентифікації користувачі не повинні розкривати свої облікові дані третім сторонам. Це дозволяє зменшити ризик витоку особистої інформації та підвищує рівень конфіденційності даних.

3) Збільшення безпеки: Використання делегованої автентифікації дозволяє впроваджувати більш надійні методи автентифікації, такі як багатофакторна аутентифікація, біометричні дані тощо. Це сприяє підвищенню рівня безпеки доступу до ресурсів та запобігає несанкціонованому використанню облікових даних.
4) Швидкий та ефективний доступ: Завдяки делегованій автентифікації користувачі можуть швидко та ефективно отримувати доступ до різних послуг та ресурсів, не витрачаючи час на повторну автентифікацію та введення облікових даних.
5) Скорочення навантаження на систему: Застосування делегованої автентифікації дозволяє системам та сервісам зосередитися на своїх основних функціях, перекладаючи процес автентифікації на провайдера ідентичності. Це допомагає скоротити навантаження на сервери та підвищує швидкість обробки запитів.
6) Розширення функціональності та інтеграція: Делегована автентифікація сприяє розширенню функціональності різноманітних сервісів та послуг шляхом інтеграції з провайдерами ідентичності. Це дозволяє користувачам використовувати єдиний набір облікових даних для отримання доступу до різноманітних ресурсів.

Загалом, делегована автентифікація відкриває шлях до зручного, безпечного та ефективного доступу до послуг та ресурсів, спрощуючи процес автентифікації та забезпечуючи більш високий рівень конфіденційності та безпеки даних користувачів.

1.3 Актуальні технології та протоколи делегованої автентифікації

Після огляду принципів та переваг делегованої автентифікації, розглянемо технології, що вже знайшли широке застосування. Перехід від принципів та переваг до існуючих технологій дозволяє побачити, яким чином концепції і принципи делегованої автентифікації перетворюються на конкретні рішення та реалізації в реальному світі.[5]

1) OAuth (Open Authorization) є відкритим протоколом авторизації, який був створений з метою забезпечення безпеки та зручності доступу до ресурсів користувача третім сторонам. Цей протокол дозволяє користувачам надавати дозвіл третім сторонам на доступ до їхніх захищених ресурсів, таких як соціальні медіа-акаунти, електронні поштові скриньки, хмарні сховища та інші, без необхідності надавати свій логін та пароль. На Рис 1.2 показано як це працює [6].

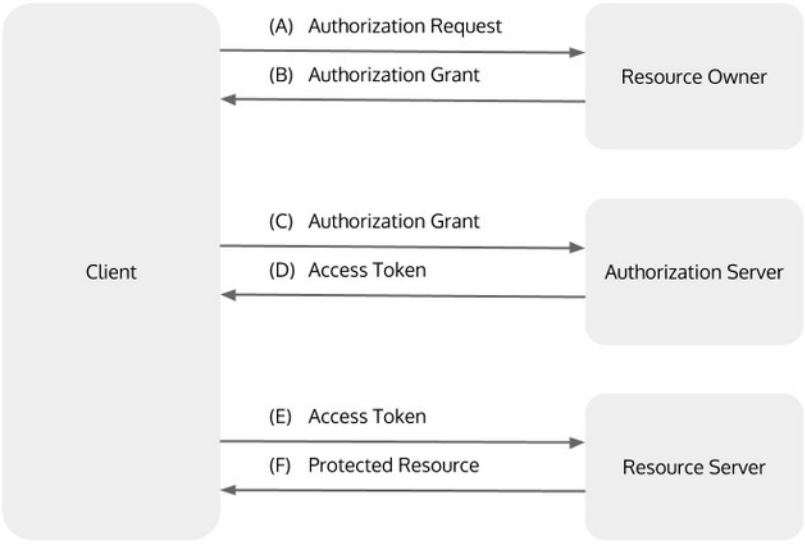

Рис 1.2. Загальна схема OAuth 2.0

2) OpenID Connect є розширенням протоколу OAuth і відіграє важливу роль у реалізації ідентифікації та автентифікації користувачів в онлайн-сервісах. Цей протокол надає стандартизований спосіб отримання інформації про ідентичність користувача, що спрощує і безпечніше здійснення делегованої автентифікації [7].

3) JSON Web Token (JWT) є стандартизованим форматом для обміну даними між сторонами в захищеній та незмінній формі. Він широко використовується для представлення токенів доступу та надає зручний механізм для передачі інформації про автентифікацію та авторизацію користувача між різними системами. На Рис 1.3 продемонстрована автентифікація за допомогою токена [8].

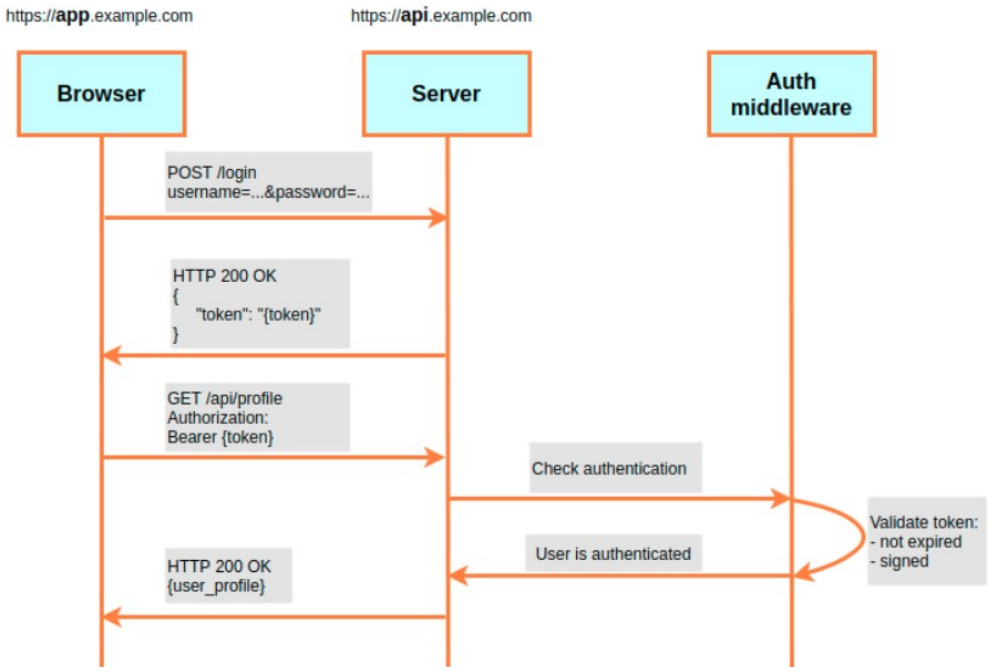

Рис 1.3. Процес автентифікації за допомогою токена

4) Security Assertion Markup Language (SAML) є протоколом, розробленим для обміну безпечною інформацією про автентифікацію та авторизацію між різними сторонами. Використовуючи мову розмітки XML, SAML дозволяє передавати повідомлення між ідентифікаційними провайдерами (Identity Providers - IdP) та постачальниками послуг (Service Providers - SP) з метою встановлення і підтвердження ідентичності користувача та їхніх прав доступу. На Рис.1.4 можна побачити як проходить процес автентифікації [9]

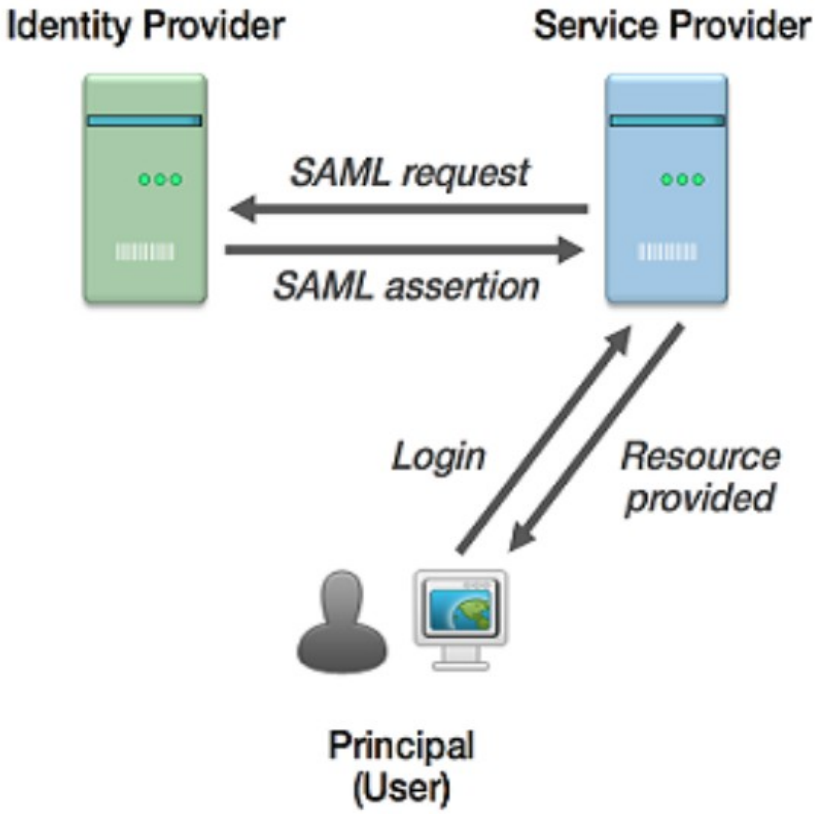

Рис 1.4. Схема процесу автентифікації SAML

5) Kerberos є протоколом для захищеної автентифікації в розподілених системах. Він розроблений з метою забезпечення безпеки ідентифікації користувачів у мережевому середовищі, де існує багато різних комп'ютерів і ресурсів. Протокол Kerberos використовує симетричне шифрування для перевірки ідентичності користувачів та забезпечує їхню автентифікацію шляхом взаємодії з трьома основними суб'єктами: клієнтом, службовим сервером та центром довіри (Key Distribution Center - KDC). KDC виконує роль центрального авторитету, що випускає та керує токенами автентифікації. Процес автентифікації в Kerberos показаний на Рис.1.5 [10].

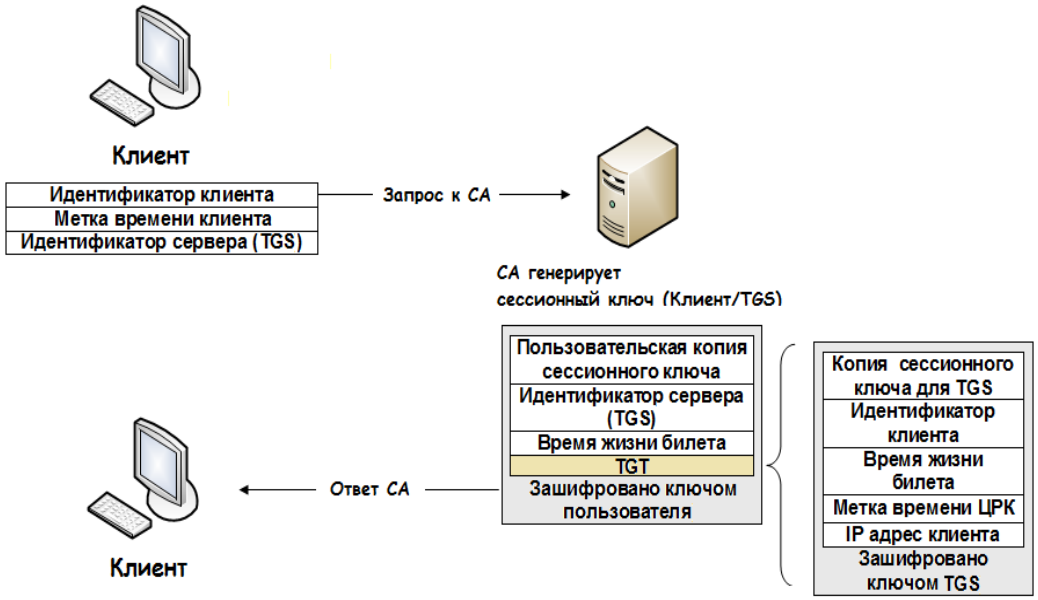

Рис.1.5 Етап автентифікації клієнта в Kerberos

6) SSL/TLS (Secure Sockets Layer/Transport Layer Security) є набором криптографічних протоколів, які забезпечують безпеку комунікації в мережі Інтернет. Ці протоколи використовуються для забезпечення конфіденційності, цілісності та аутентифікації даних, що передаються між клієнтом та сервером. В контексті делегованої автентифікації, SSL/TLS відіграють важливу роль у забезпеченні безпеки передачі інформації, включаючи ідентифікаційні дані та токени доступу [11].
7) FIDO (Fast Identity Online): Ця технологія забезпечує сильну аутентифікацію за допомогою біометричних даних або фізичних токенів. FIDO дозволяє делегувати автентифікацію на спеціальні пристрої або провайдерів ідентичності, що забезпечують високий рівень безпеки. Ось наглядно як це працює Рис. 1.6 [12].

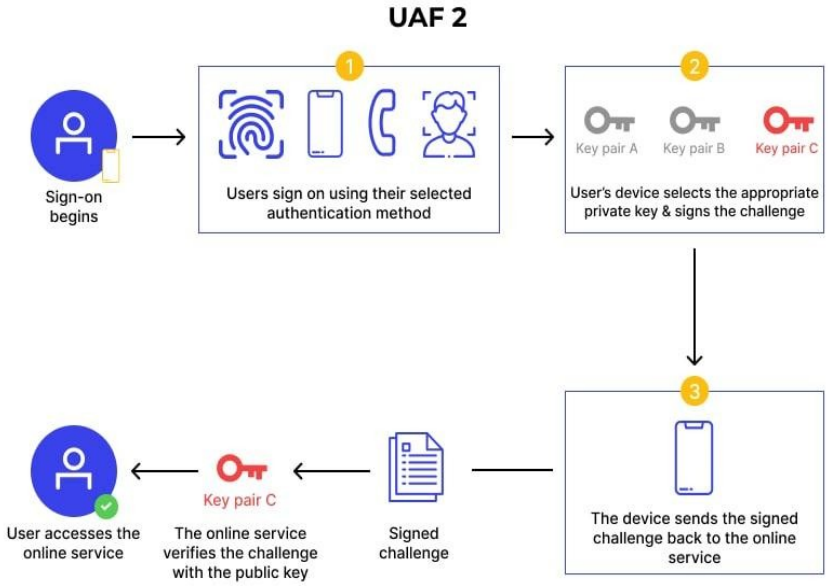

Рис. 1.6. Процес автентифікації за допомогою FIDO

8) WebAuthn: Ця веб-стандартна технологія дозволяє сильну аутентифікацію без використання паролів. Вона базується на використанні публічного ключа криптографії та біометричних даних для підтвердження ідентичності користувача. Детально описано як ця технологія працює на Рис.1.7 [13].

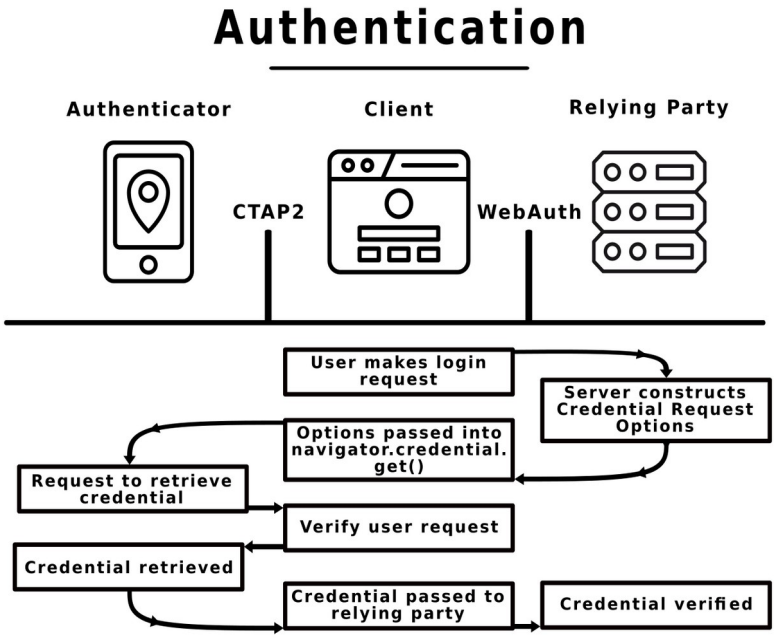

Рис.1.7. Процес автентифікації WebAuthn

9) Shibboleth: Ця ідентифікаційна рамка дозволяє делегувати автентифікацію в університетських та дослідницьких середовищах. Shibboleth використовує протоколи SAML та OAuth для обміну токенами та делегування автентифікації на провайдерів ідентичності. Чудовий приклад зображений на Рис.1.8,як приблизно проходить цей процес [14].

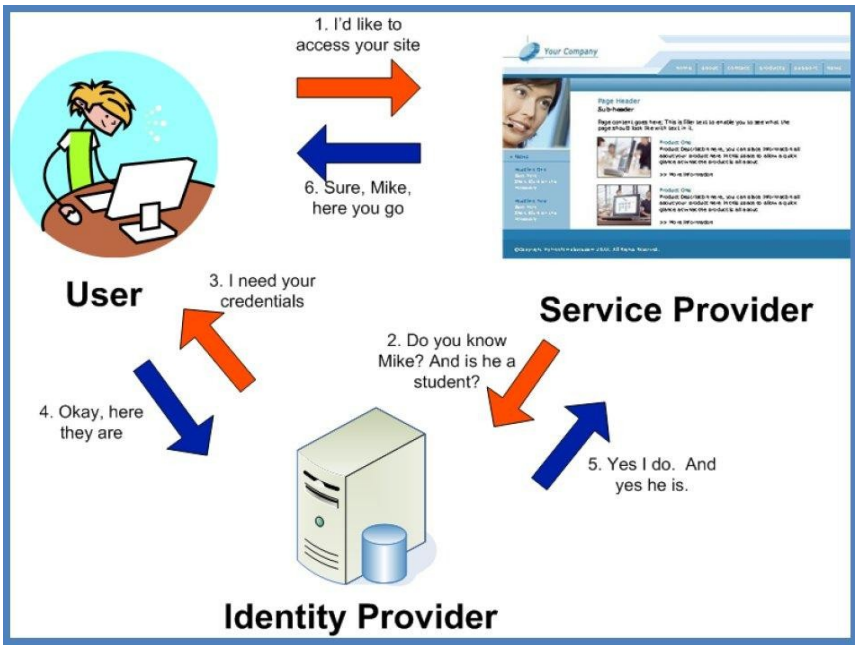

Рис.1.8. Операційна схема Shibboleth

10) Active Directory Federation Services (ADFS): Це рішення від Microsoft, яке дозволяє делегувати автентифікацію між різними доменами та сервісами, використовуючи протоколи SAML та OAuth. Послідовність та як взагалі проходить процес видно чудово на Рис.1.9 [15].

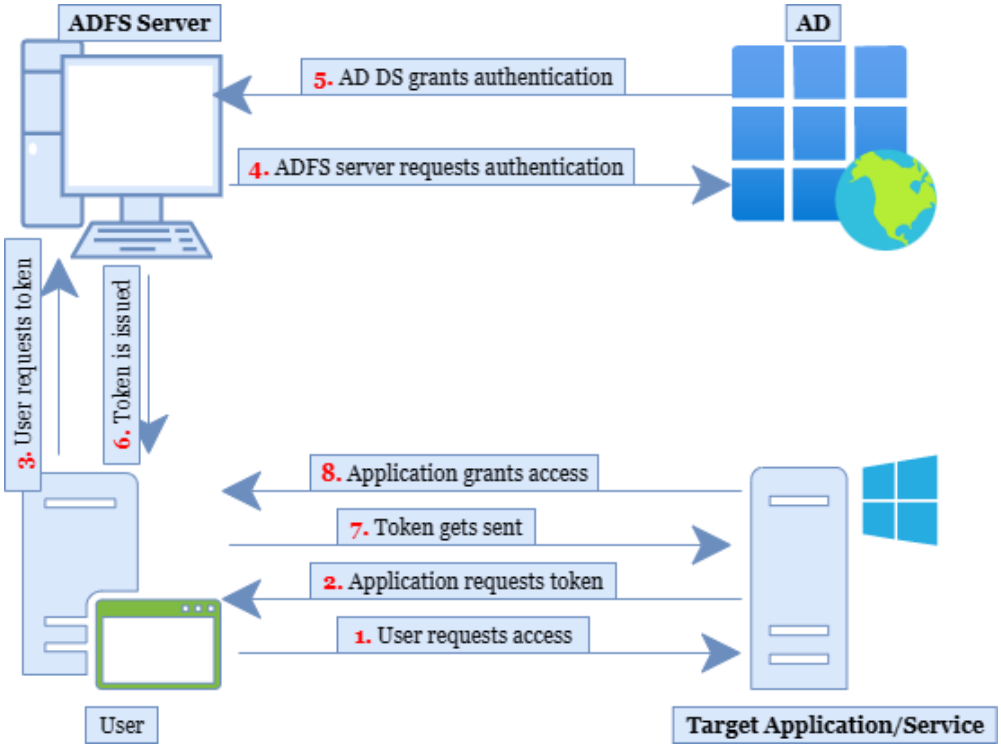

Рис.1.9. Робочий процес для систем на основі ADFS

Завдяки постійному розвитку інтернет-технологій і зростанню потреб користувачів у безпеці та зручності, існує ряд ефективних технологій та протоколів в галузі делегованої автентифікації. Ці інструменти надають можливість користувачам забезпечувати доступ до своїх ресурсів третім сторонам, зберігаючи при цьому безпеку і контроль над своїми ідентифікаційними даними. Вони відкривають шлях до сучасних інновацій та дозволяють ефективно управляти ідентичністю та доступом, забезпечуючи надійну і захищену автентифікацію для всіх користувачів.

1.4 Перспективні технології та напрямки розвитку в галузі делегованої автентифікації

Перспективні технології та напрямки розвитку в сфері делегованої автентифікації зосереджені на забезпеченні найвищих рівнів безпеки, надійності та зручності для користувачів. Ці напрямки включають використання нових методів ідентифікації, розширення функціональності, розробку стандартів і протоколів, а також застосування нових підходів до зберігання та обміну ідентифікаційними даними. Використання біометричних

технологій, таких як розпізнавання обличчя, відбитків пальців та голосу, забезпечують високий рівень безпеки та зручності. Багатофакторна автентифікація, яка поєднує різні елементи ідентифікації, такі як паролі, одноразові коди та фізичні пристрої, ще більше підвищує надійність процесу ідентифікації. Децентралізовані та блокчейн-рішення виводять на новий рівень безпеку та конфіденційність зберігання та обміну ідентифікаційними даними. Крім того, важливим напрямком розвитку є стандартизація та інтеграція різних протоколів і стандартів у сфері делегованої автентифікації. Це забезпечить сумісність та інтероперабельність між різними системами та спростить процес впровадження та використання делегованої автентифікації. Загалом, перспективні технології та напрямки розвитку у сфері делегованої автентифікації спрямовані на підвищення безпеки, зручності та ефективності процесів ідентифікації користувачів у цифровому світі. Інновації в біометричних технологіях, багатофакторній автентифікації, блокчейн-рішеннях та стандартизації дозволять створити надійні та зручні системи, які відповідатимуть вимогам сучасних користувачів та компаній. Перспективні технології та напрямки розвитку в галузі делегованої автентифікації орієнтовані на покращення безпеки, зручності та ефективності процесу ідентифікації користувачів [16]. Нижче розглянемо деякі з цих технологій більш детально:

1) Біометричні технології: Застосування біометричних методів ідентифікації, таких як розпізнавання обличчя, відбитків пальців, сканування радужної оболонки ока тощо, має великий потенціал для покращення безпеки та зручності в делегованій автентифікації. Ці технології дозволяють використовувати фізичні характеристики користувача як унікальні ідентифікатори, що забезпечує високий рівень безпеки. Види біометричних технологій добре показано на Рис.1.10[17].

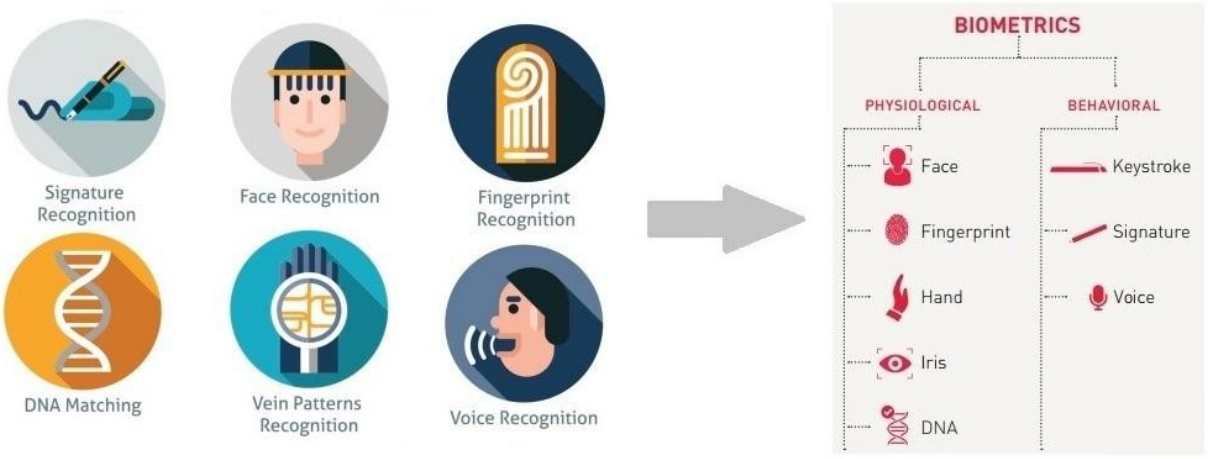

Рис.1.10. Види біометричних технологій

2) Мультифакторна автентифікація (MFA): Мультифакторна автентифікація використовує комбінацію різних факторів ідентифікації, таких як пароль, одноразовий код, фізичний пристрій або біометричні

дані. Впровадження MFA забезпечує вищий рівень безпеки, оскільки зламування одного фактора не дозволить отримати доступ до системи. Переваги різних методів MFA показаний у табл.1.3.

Табл.1.3.Переваги факторів ідентифікації

Фактори ідентифікації	Переваги
Паролі	Знайомий метод автентифікації, недорогий
Одноразові коди	Високий рівень безпеки, одноразові та складні для вгадування
Фізичні пристрої	Двофакторна аутентифікація, високий рівень безпеки, зручний для використання
Біометричні дані	Унікальність ідентифікаторів, високий рівень безпеки

3) Децентралізовані ідентичності: Децентралізовані ідентичності базуються на технології блокчейн, де користувачі мають повний контроль над своїми ідентифікаційними даними та можуть надавати доступ до них за необхідності. Це забезпечує високий рівень приватності та безпеки, оскільки користувачі самостійно управляють своїми ідентичностями та визначають, кому та в якому обсязі вони надають доступ до своїх даних. На Рис.1.11 зображено пошагово як працює блокчейн.

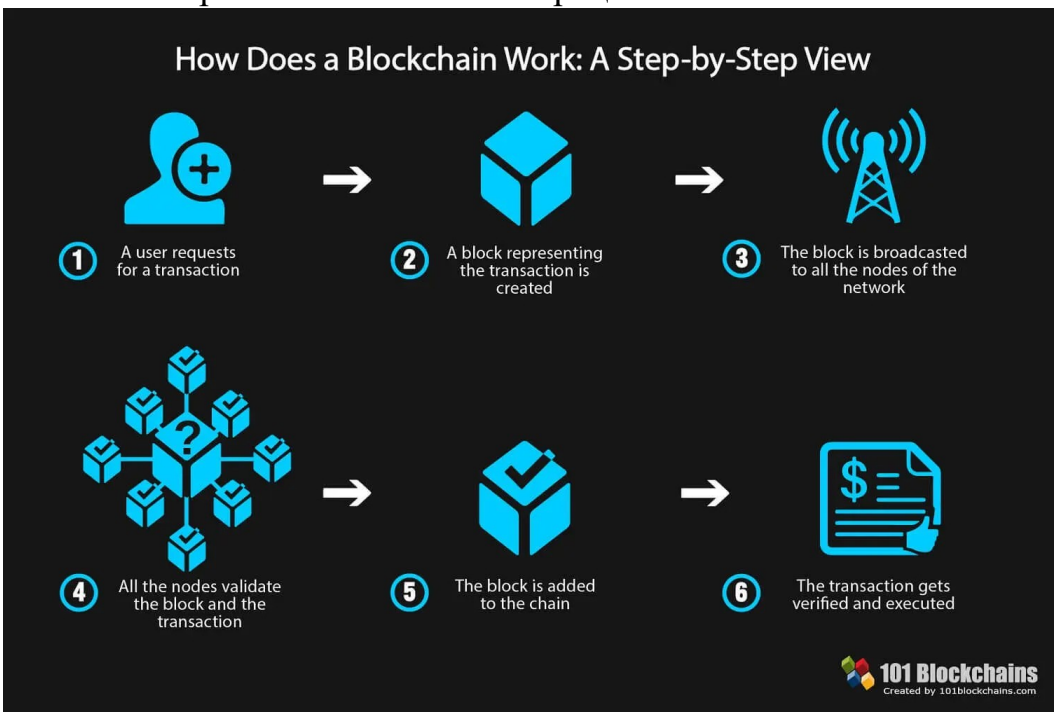

Рис.1.11. Як працює блокчейн

4) Використання стандартів та протоколів: Стандартизація грає важливу роль у розвитку делегованої автентифікації. Розвиток та удосконалення протоколів, таких як OAuth, OpenID Connect, SAML та інші, сприяють забезпеченню сумісності та стандартизації взаємодії між різними системами автентифікації. Це дозволяє розробникам швидше та ефективніше впроваджувати делеговану автентифікацію у своїх додатках та послугах. Нижче в табл.1.4 наведено список стандартів та протоколів.

Табл.1.4. Стандарти та протоколи в делегованій автентифікації

Стандарти та протоколи	Опис
OAuth	Протокол авторизації для делегованої автентифікації
OpenID Connect	Стандарт для безпечної автентифікації та обміну ідентифікаційними даними
SAML	Мова обміну повідомленнями для автентифікації між сторонами
FIDO2	Стандарт аутентифікації на основі відкритих стандартів

5) Розширення підтримки провайдерів: Постійне розширення списку провайдерів делегованої автентифікації є важливим напрямком розвитку. Це означає підтримку нових соціальних мереж, ідентичнісних платформ та інших сервісів, що дозволяють користувачам використовувати єдині облікові записи для автентифікації в різних системах.

В цілому, перспективні технології та напрямки розвитку в галузі делегованої автентифікації спрямовані на покращення безпеки, зручності та ефективності процесу ідентифікації користувачів. Інновації у вищезгаданих областях сприятимуть створенню надійних та зручних систем автентифікації, які відповідають потребам сучасного цифрового середовища.

РОЗДІЛ 2.СЦЕНАРІЇ ЗАСТОСУВАННЯ СИСТЕМ ДЕЛЕГОВАНОЇ АВТЕНТИФІКАЦІЇ

2.1 Автентифікація на веб-сторінках

Автентифікація на веб-сторінках є важливим аспектом для забезпечення безпеки та конфіденційності в онлайн-середовищі. У сучасному світі, коли користувачі взаємодіють з багатьма веб-сервісами та додатками, необхідність використання різних облікових записів та реєстрації на кожному з них стає обтяжливою і неефективною.

Саме тут системи делегованої автентифікації набувають значення. Ці системи дозволяють користувачам увійти на веб-сторінки та використовувати їх послуги за допомогою облікового запису, який вже мають у відповідних провайдерах. Архітектура систем делегованої автентифікації передбачає, що веб-сторінка використовує стороннього постачальника ідентичності для перевірки та автентифікації користувачів. Такий підхід дозволяє спростити процес автентифікації, забезпечити одноразову реєстрацію для кількох веб-сервісів та полегшити використання для кінцевих користувачів.

Автентифікація на веб-сторінках використовує різні архітектурні підходи та принципи, включаючи системи делегованої автентифікації. Ці системи дозволяють веб-сторінкам автентифікувати користувачів за допомогою сторонніх провайдерів ідентичності, зменшуючи необхідність в утриманні та керуванні власними системами автентифікації.

Архітектура системи делегованої автентифікації для веб-сторінок зазвичай включає компоненти наведені в табл.2.1:

Табл.2.1.Архітектура системи делегованої автентифікації для веб-сторінок

Компонент	Опис	Взаємодія
Веб-сторінка (клієнт)	Веб-сайт або додаток, що потребує автентифікації	Взаємодія з сервісом автентифікації, сховищем токенів, захищеними ресурсами
Ідентифікаційний провайдер	Сервіс, що забезпечує процес автентифікації	Перевірка облікових даних, генерація токенів
Сервіс автентифікації	Забезпечує комунікацію між веб-сторінкою та ідентифікаційним	Перенаправлення користувача, отримання токенів

Компонент	Опис	Взаємодія
	провайдером	
Сховище токенів	Безпечне сховище для зберігання токенів	Зберігання токенів, використання при запитах до захищених ресурсів
Захищені ресурси	Ресурси або послуги, що вимагають автентифікації	Доступ до ресурсів після успішної автентифікації

Принципи систем делегованої автентифікації включають:

1)Розподілена автентифікація: Замість того, щоб кожен веб-сайт або додаток мати власну систему автентифікації, використовуються сторонні провайдери ідентичності, які спрощують процес автентифікації для користувачів і зменшують навантаження на веб-сторінки.
2)Розширення можливостей: Системи делегованої автентифікації надають можливість використовувати різні провайдери ідентичності, такі як соціальні мережі або корпоративні системи, що розширює варіанти автентифікації для користувачів.
3)Забезпечення безпеки: Використання протоколів автентифікації, які використовують шифрування та механізми безпеки, дозволяє забезпечити конфіденційність та цілісність ідентичності користувача під час передачі даних між веб-сторінкою та провайдером ідентичності.
4)Спрощена інтеграція: Системи делегованої автентифікації надають стандартизовані протоколи, що спрощують процес інтеграції між веб-сторінками та провайдерами ідентичності. Це дозволяє розробникам швидше впроваджувати автентифікацію на своїх веб-сторінках.

Загалом, автентифікація на веб-сторінках базується на архітектурі та принципах делегованої автентифікації, що дозволяє забезпечити безпеку, зручність та розширені можливості для користувачів та розробників.

Після розгляду архітектури та принципів систем делегованої автентифікації для веб-сторінок, варто звернутися до оцінки плюсів та мінусів використання таких систем на веб-сторінках. Оцінка переваг та обмежень допоможе нам краще зрозуміти, як ці системи впливають на зручність, безпеку та ефективність автентифікації користувачів.

Плюси та мінуси використання систем делегованої автентифікації на веб-сторінках надені в табл.2.2:

Табл.2.2. Переваги та недоліки делегованої автентифікації на веб-сторінках

Плюси систем делегованої автентифікації	Мінуси систем делегованої автентифікації
Зручність для користувачів	Залежність від сторонніх провайдерів
Зменшення ризику витоку облікових даних	Вплив на конфіденційність даних
Загальна безпека	Складність інтеграції і підтримки
Розширені можливості	Зростаюча складність безпеки
Спрощений розподіл ресурсів	Складність управління доступом

Враховуючи ці мінуси, веб-сторінкам слід уважно зважити на переваги та недоліки використання систем делегованої автентифікації та вжити відповідні заходи безпеки та контролю для забезпечення надійності та ефективності системи автентифікації.

Після розгляду плюсів та мінусів використання систем делегованої автентифікації на веб-сторінках, перейдемо до прикладів таких систем автентифікації. Двом широко використовуваним протоколам, що дозволяють реалізувати делеговану автентифікацію, є OAuth та OpenID Connect.

Табл.2.3 може візуально відобразити різницю та спільні аспекти між OAuth та OpenID Connect, допомагаючи краще розуміти їх.

Табл.2.3.Основні аспекти OAuth та OpenID Connect.

Особливості	OAuth	OpenID Connect
Тип протоколу	Протокол авторизації	Розширення протоколу OAuth
Мета	Надання стороннім додаткам обмеженого доступу до користувачівих ресурсів без розкриття облікових даних	Підтвердження ідентичності користувача та отримання додаткової інформації про нього
Використання	Інтеграція зі сторонніми провайдерами автентифікації, такими як Google, Facebook, Twitter	Забезпечення стандартизованої схеми автентифікації та отримання інформації про користувача

Особливості	OAuth	OpenID Connect
Механізм доступу	Використання автентифікаційного токена, виданого веб-сторінкою	Використання JSON Web Tokens (JWT) для передачі інформації про ідентичність
Отримання даних	Обмежений доступ до користувацьких ресурсів на веб-сторінках	Структуровані дані про користувача, такі як ім'я, електронна адреса, фотографія тощо
Розширення	Немає	Розширення протоколу OAuth
Безпека	Забезпечення обмеженого доступу до користувацьких ресурсів без розкриття облікових даних	Захист ідентичності та конфіденційності даних за допомогою JWT
Використання веб-сторінками	Широке використання для інтеграції зі сторонніми провайдерами автентифікації	Використовується для підтвердження ідентичності та отримання даних користувача
Розширення можливостей	Надання обмеженого доступу до ресурсів через API	Отримання структурованих даних про користувача для розширення функціональності
Переваги	Зручність для користувачів, безпека облікових даних	Підтвердження ідентичності, отримання корисної інформації про користувача
Недоліки	Ризик доступу сторонніх додатків до обмежених користувацьких ресурсів	Залежність від провайдерів ідентичності, можлива складність налаштування

Ці два протоколи, OAuth і OpenID Connect, є потужними інструментами для реалізації делегованої автентифікації на веб-сторінках. Вони спрощують процес автентифікації користувача, забезпечують безпеку обміну даними та дозволяють веб-сторінкам інтегруватися зі сторонніми провайдерами автентифікації для поліпшення користувацького досвіду.

2.2 Системи делегованої автентифікації для надання цифрових послуг

Системи делегованої автентифікації займають центральне місце в забезпеченні безпеки і зручності використання цифрових послуг. Особливо в сферах фінансових установ і державних органів, де існує високий рівень конфіденційності та важливість запобігання несанкціонованому доступу, системи делегованої автентифікації мають вирішальне значення. Ці системи дозволяють користувачам використовувати свої облікові записи з одного сервісу для автентифікації на інших пов'язаних сервісах, забезпечуючи одночасно зручність та безпеку. Огляд системи делегованої автентифікації у різних застосуваннях, таких як фінансові установи та державні органи, виявляє різноманітність та важливість цього підходу до забезпечення безпеки та зручності доступу до ресурсів. Нижче в табл.2.4 наведено огляд системи делегованої автентифікації у цих галузях:

Табл.2.4.Системи делегованої автентифікації в фінансових установах та державних органах

Застосування	Фінансові установи	Державні органи
Тип послуг	Безпека фінансових операцій, доступ до банківських рахунків	Електронні послуги, захист особистих даних громадян
Облікові записи	Використання облікових записів на сторонніх платформах для автентифікації	Використання електронних ідентифікаційних засобів
Зручність	Спрощений процес входу, уникнення необхідності в запам'ятовуванні багатьох облікових записів і паролів	Ефективна взаємодія з державними органами
Безпека	Високий рівень захисту фінансових операцій, аутентифікаційні механізми ідентичнісного провайдера	Захист персональних даних громадян, високий рівень конфіденційності
Переваги	Зручність, полегшений доступ до ресурсів	Ефективність, висока безпека даних
Недоліки	Ризик доступу сторонніх додатків до фінансових ресурсів	Залежність від електронних ідентифікаційних засобів, необхідність належного захисту даних

Принцип роботи делегованої автентифікації у фінансових установах показано на Рис.2.1.

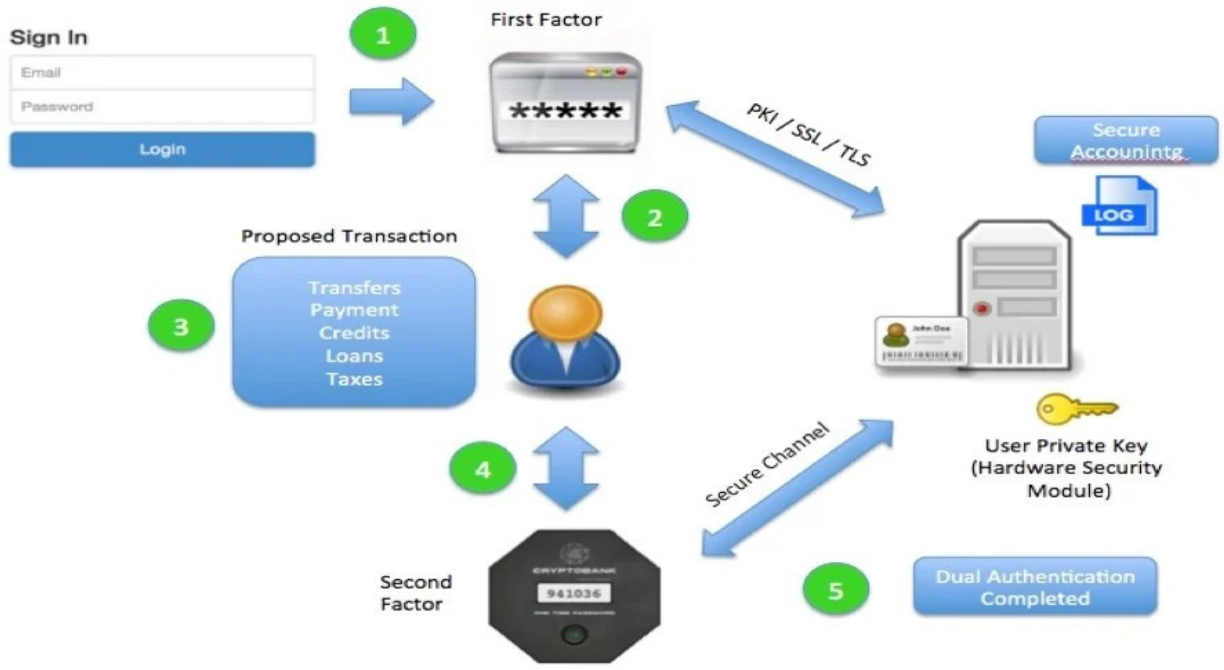

Рис.2.1.Делегована автентифікація у фінансових установах

Огляд системи делегованої автентифікації у різних застосуваннях, таких як фінансові установи та державні органи, вказує на різноманітність та важливість цього підходу до забезпечення безпеки та зручності доступу до ресурсів.[18] Для кращого розуміння архітектури, принципів та особливостей використання систем автентифікації у цих галузях, розглянемо наступне:

1. Архітектура системи делегованої автентифікації в фінансових установах та державних органах ґрунтується на клієнт-серверній моделі. Система складається з наступних компонентів:

- Клієнт: Веб-сторінка або додаток, що використовується користувачем для доступу до ресурсів.
- Ідентичнісний провайдер: Зовнішня система або служба, що надає автентифікаційні послуги та перевіряє ідентичність користувача.
- Автентифікаційний токен: Маркер, що містить інформацію про автентифікованого користувача і передається клієнту для доступу до ресурсів.
- Сервер: Обробляє запити від клієнтів, перевіряє автентифікаційний токен і надає доступ до ресурсів.

2. Принципи безпеки системи автентифікації в фінансових установах та державних органах:

- Високий рівень безпеки: Використання сильної аутентифікації, включаючи сильні паролі, двофакторну аутентифікацію та біометричні методи.
- Шифрування даних: Застосування шифрування для захисту конфіденційності даних під час передачі і збереження.
- Дотримання стандартів і правил: Використання встановлених стандартів і правил безпеки, таких як PCI DSS або GDPR.
- Моніторинг і аудит: Постійний моніторинг системи автентифікації та проведення аудиту для виявлення незвичайної активності та потенційних вразливостей.

3. Особливості використання автентифікації в фінансових установах та державних органах:

- Багаторівневі методи авторизації: У фінансових установах використовуються різні рівні авторизації, включаючи додаткові фактори, які підвищують безпеку доступу до ресурсів.
- Захист конфіденційності особистої інформації: У державних органах велике значення має захист особистих даних громадян та дотримання відповідних регуляторних вимог і стандартів.
- Використання авторитетних джерел ідентичності: У державних органах важливо перевіряти ідентичність користувачів за допомогою надійних джерел, що гарантує достовірність даних, що обробляються.

Узагальнюючи, у фінансових установах та державних органах використання систем делегованої автентифікації вимагає впровадження багаторівневих методів авторизації, забезпечення конфіденційності особистих даних та використання авторитетних джерел ідентичності. Це допомагає забезпечити безпеку, надійність та довіру у процесі автентифікації користувачів у цих галузях.

Впровадження систем автентифікації у фінансових установах та державних органах має свої плюси, мінуси та підводні камені. Розглянемо це детальніше.

Плюси:

1) Висока безпека: Системи автентифікації забезпечують сильну аутентифікацію та шифрування даних, що гарантує безпеку конфіденційної інформації в фінансових установах та державних органах.
2) Зручність для користувачів: Використання існуючих облікових даних спрощує процес автентифікації та уникнення створення нових облікових записів.

3) Ефективність та автоматизація: Системи автентифікації дозволяють автоматизувати процеси перевірки та ідентифікації користувачів, що сприяє швидкості та ефективності.
4) Відповідність нормативам: Впровадження систем автентифікації допомагає відповідати вимогам щодо захисту персональних даних та конфіденційності.

Мінуси:

1) Складність впровадження: Впровадження може бути складним у великих установах зі складною інфраструктурою.
2) Вартість: Впровадження може вимагати значних фінансових зусиль, що може бути обтяжливим для організацій з обмеженими бюджетами.
3) Високі вимоги до інфраструктури: Для успішної роботи системи автентифікації необхідна надійна та потужна інфраструктура.
4) Потреба в навчанні користувачів: Впровадження нової системи вимагає навчання користувачів та введення нових процедур.
5) Потенційні проблеми з безпекою: Недоліки в системі можуть призвести до проблем з безпекою, що потребує постійного оновлення технологій та процедур.

Підводні камені:

1) Регуляторні вимоги: Відповідність регуляторним вимогам та стандартам безпеки може бути викликом, і необхідно забезпечити відповідність системи автентифікації всім необхідним вимогам.
2) Сумісність з існуючими системами: Інтеграція нової системи автентифікації з існуючими системами та забезпечення сумісності може потребувати додаткових зусиль та розробки спеціальних рішень для вирішення технічних викликів.
3) Соціальне прийняття: Переконання користувачів щодо важливості та безпеки системи автентифікації може бути важливим завданням, оскільки недовіра або незадоволення користувачів може обмежити використання системи.
4) Технічні проблеми: Непередбачені помилки, проблеми зі сумісністю або швидкодією системи можуть виникнути під час впровадження, тому необхідно проводити відповідне тестування та мати плани на випадок технічних проблем.

Впровадження систем автентифікації в галузі фінансових установ та державних органів має як позитивні, так і негативні аспекти. Переваги впровадження таких систем включають забезпечення високого рівня безпеки, захисту персональних даних та можливість використання сучасних методів аутентифікації, таких як двофакторна аутентифікація і біометричні дані. Вони також сприяють поліпшенню доступу до ресурсів та послуг,

спрощують процеси ідентифікації та авторизації, а також сприяють впровадженню стандартів безпеки та регуляторних вимог. Проте, існують також деякі недоліки та підводні камені. Впровадження таких систем вимагає детального вивчення регуляторної рамки та відповідності вимогам стандартів безпеки. Інтеграція з існуючими системами та забезпечення сумісності може стати складною задачею. Деякі користувачі можуть виявляти недовіру до нової системи та бути несхвальними до передачі своїх персональних даних. Також, впровадження нової системи може зіткнутися з технічними проблемами та вимагати значних витрат та ресурсів.

Для успішного впровадження систем автентифікації в галузі фінансових установ та державних органів, необхідно ретельно вивчити всі аспекти впливу, проводити тестування та забезпечувати відповідність регуляторним вимогам. Крім того, важливо враховувати соціальний аспект та проводити пояснювальну роботу серед користувачів для підвищення довіри та свідомого використання системи. Забезпечення належного фінансування, планування резервного копіювання та навчання персоналу також є ключовими чинниками успішного впровадження.

В цілому, при належному підході та врахуванні важливих аспектів, впровадження систем автентифікації може принести значну користь фінансовим установам та державним органам, покращуючи безпеку, ефективність та доступність їхніх послуг.

РОЗДІЛ 3. СИСТЕМИ АВТЕНТИФІКАЦІЇ BANKID, MOBILEID ТА СИСТЕМИ ДІЯ

3.1 Огляд системи автентифікації BankID

BankID - це система автентифікації, яка використовується у багатьох країнах для ідентифікації користувачів у фінансових установах та державних органах. Давайте розглянемо основні аспекти архітектури та принципів роботи цієї системи[19].

Архітектура BankID базується на клієнт-серверній моделі, де клієнтська сторона взаємодіє з сервером для автентифікації користувача показано на Рис.3.1. Основні компоненти системи наведені в табл.3.1:

Табл.3.1. Основні компоненти архітектури BankID та їх ролі

Компонент	Опис ролі та функціональності
Клієнтська сторона	Клієнтська сторона представляє собою програмний інтерфейс, який взаємодіє з користувачем. Вона надає можливість користувачеві ввести свої автентифікаційні дані та виконати запит на автентифікацію через серверну сторону.
Серверна сторона	Серверна сторона відповідає за обробку запитів на автентифікацію від клієнтської сторони. Вона перевіряє коректність та достовірність наданих автентифікаційних даних та виконує необхідні перевірки безпеки перед наданням доступу до системи.
Протоколи комунікації	Протоколи комунікації визначають спосіб передачі даних між клієнтською та серверною сторонами. Вони включають у себе правила та формати для обміну повідомленнями, шифрування та забезпечення цілісності даних під час передачі.
База даних	База даних є централізованим сховищем, де зберігаються дані про користувачів, їх автентифікаційні дані та інша важлива інформація, необхідна для процесу автентифікації. Вона забезпечує доступ до необхідних даних для серверної сторони під час обробки запитів.
Криптографічні методи	Криптографічні методи використовуються для забезпечення безпеки даних під час процесу автентифікації. Вони включають у себе шифрування даних, хешування для перевірки цілісності та цифрові підписи для підтвердження автентичності.

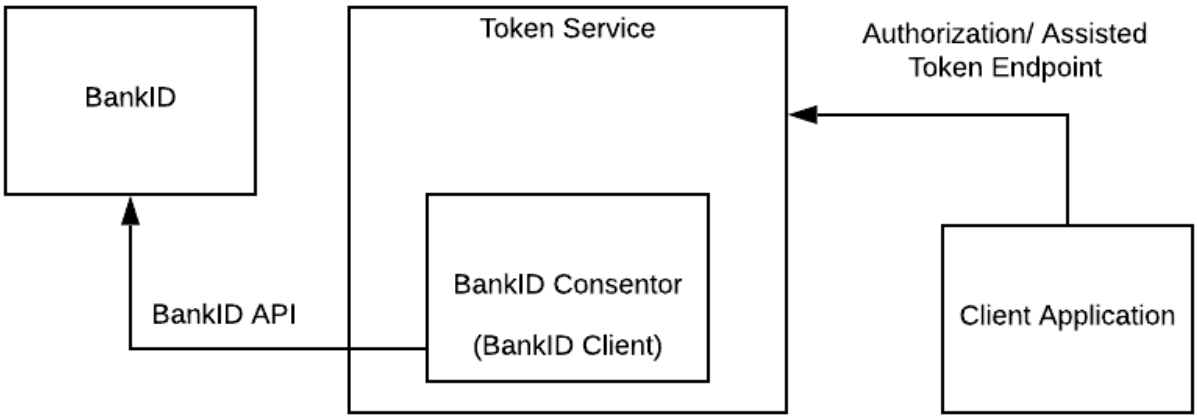

Рис.3.1. Огляд інтеграції BankID

Принципи роботи системи BankID базуються на сильній аутентифікації та безпеці даних. Ці принципи є основою для забезпечення надійності, конфіденційності та цілісності процесу автентифікації. Основні принципи роботи системи наведені в табл.3.2:

Табл.3.2. Основні принципи роботи системи BankID

Принципи	Опис
Сильна аутентифікація	Вимога до користувачів пройти сильну аутентифікацію для підтвердження їх ідентичності. Це може включати двофакторну аутентифікацію, біометричні дані або використання апаратних пристроїв.
Захист даних	Використання шифрування для захисту передачі та зберігання конфіденційних даних. Застосування шифрування протоколами, такими як SSL/TLS, та шифрування даних на серверах.
Надійність та доступність	Забезпечення високої надійності та доступності системи за допомогою резервування серверів, розподіленого зберігання даних, резервного копіювання та відновлення, а також механізмів моніторингу та виявлення неполадок.
Законність та відповідність	Дотримання вимог законодавства та нормативних актів, що регулюють обробку персональних даних та забезпечують конфіденційність інформації користувачів. Відповідність вимогам регуляторів та органів влади.

Загалом, архітектура та принципи роботи системи BankID забезпечують безпеку, надійність та ефективність процесу автентифікації у фінансових установах та державних органах. Ця система дозволяє забезпечити високий рівень захисту персональних даних та зручність для користувачів під час отримання доступу до важливих ресурсів та послуг.

Застосування та особливості використання BankID [20]:

1. Онлайн-банкінг: BankID використовується у фінансових установах для автентифікації користувачів, які отримують доступ до своїх банківських рахунків через онлайн-платформу, яка зображена на Рис.3.2. Завдяки BankID користувачі можуть безпечно і зручно виконувати фінансові операції, переказувати кошти, оплачувати рахунки та отримувати фінансову інформацію.

Рис.3.2.Онлайн-платформа BankID

2. Електронна ідентифікація: BankID використовується як електронний ідентифікатор, який показаний на Рис.3.3, що підтверджує особу користувача при взаємодії з різними онлайн-сервісами. Це може бути доступ до державних послуг, електронної пошти, електронної комерції та інших онлайн-ресурсів, де необхідно підтвердження особи.

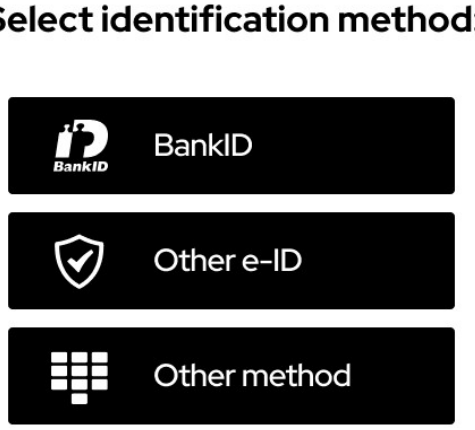

Рис.3.3. Візуалізація процесу електронної ідентифікації

3. Електронний підпис: BankID також може використовуватися для надання електронного підпису, що має правову силу. Користувачі можуть підписувати електронні документи, контракти, заявки та інші юридично значущі документи без необхідності фізичного присутності, як показано на Рис.3.4.

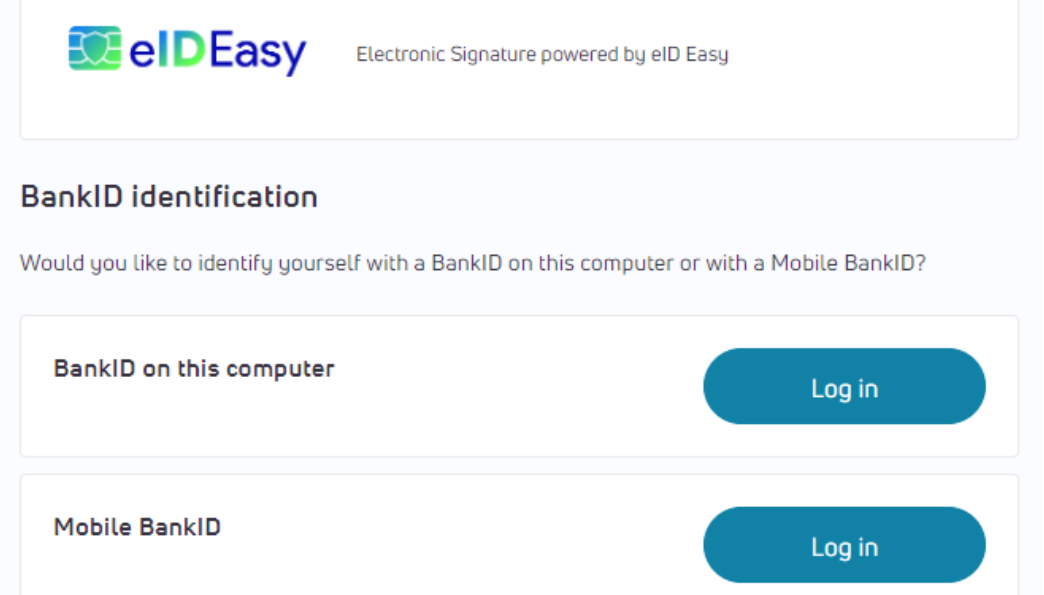

Рис.3.4. Ілюстрація електронного підпису

4. Захист персональних даних: Однією з особливостей BankID є високий рівень захисту персональних даних користувачів. Всі дані, що передаються під час процесу автентифікації, шифруються і захищаються від несанкціонованого доступу. Це забезпечує конфіденційність та безпеку інформації, що обмінюється між користувачем і ресурсами, що використовують BankID. Схема наведена на Рис.3.5.

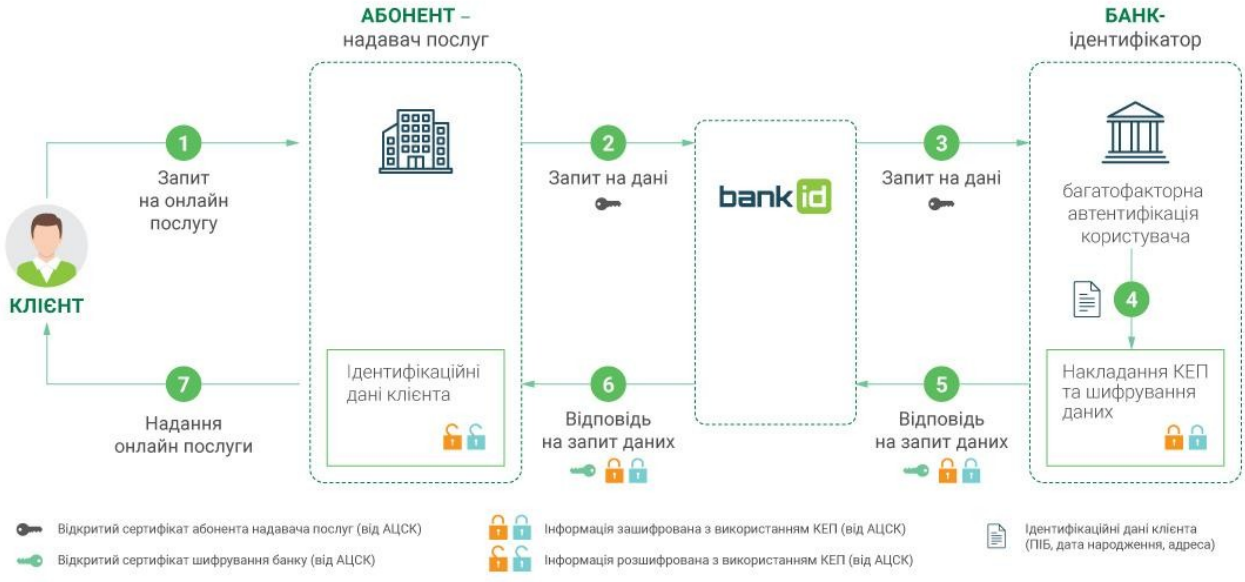

Рис.3.5.Захист персональних даних в системі BankID

5. Мобільна доступність: BankID може бути доступним як на веб-сторінках, так і у вигляді мобільних додатків. Це дозволяє користувачам зручно використовувати систему на різних пристроях, таких як смартфони і планшети. Мобільні додатки BankID забезпечують додаткову безпеку через використання біометричних данних, таких як відбитки пальців або сканування обличчя, що проілюстрований на Рис.3.6, для підтвердження ідентичності користувача.

Рис.3.6.Сканування обличчя в BankID

6. Широке застосування: BankID використовується не лише у фінансових установах та державних органах, але і в інших сферах, як показано на Рис.3.7, які потребують надійної автентифікації. Це можуть бути онлайн-ресурси з медичною інформацією, освітні платформи, системи онлайн-бронювання та багато інших.

Рис.3.7.Сфери використання BankID

В цілому, система BankID забезпечує безпеку, зручність та надійність при автентифікації користувачів у різних сферах. Її використання дозволяє забезпечити захист персональних даних, ефективну ідентифікацію та спрощення процесів, пов'язаних з отриманням доступу до ресурсів та послуг.

Застосування та особливості використання системи BankID у фінансових установах та державних органах надають ряд переваг, але також можуть мати й недоліки, які наведено у табл.3.3.

Табл.3.3. Переваги і недоліки системи BankID

Переваги використання системи BankID	**Недоліки використання системи BankID**
Високий рівень безпеки	Залежність від зв'язку з Інтернетом
Зручність для користувачів	Залежність від ідентичнісних провайдерів
Широке застосування	Ризик компрометації акаунта
Довіра та авторитет	Вартість впровадження
Ефективність та часові ресурси	Питання приватності даних

BankID є системою автентифікації, яка має стабільну архітектуру та працює на основі принципів безпеки і надійності. Її застосування в фінансових установах та державних органах дозволяє забезпечити високий рівень захисту персональних даних та зручність для користувачів при доступі до важливих ресурсів і послуг. Особливості використання BankID полягають у співробітництві з ідентичнісними провайдерами, які підтверджують ідентичність користувача. При розгляді системи BankID варто враховувати як переваги, так і недоліки. Переваги включають забезпечення безпеки, надійності та ефективності процесу автентифікації, а також спрощення доступу до ресурсів та послуг для користувачів. З іншого боку, недоліки системи BankID включають залежність від Інтернет-підключення, обмеження доступу для користувачів без акаунтів в ідентичнісних провайдерах, ризик компрометації акаунтів, вартість впровадження та питання приватності даних. Враховуючи ці фактори, важливо здійснювати належне управління ризиками та вживати заходів безпеки для забезпечення максимальної захищеності та конфіденційності даних при використанні системи BankID.

3.2 Огляд системи автентифікації MobileID

MobileID є системою автентифікації, яка заснована на використанні мобільних пристроїв, таких як смартфони або планшети, для підтвердження ідентичності користувачів. Ця система надає безпечний та зручний спосіб доступу до різних ресурсів та послуг, вимагаючи мінімальних зусиль з боку користувача [21].

Архітектура системи MobileID включає наступні основні компоненти, наведені в табл.3.4:

Табл.3.4.Основні компоненти та їх опис у системі MobileID

Компонент	Опис
Користувач	Кінцевий користувач, який використовує мобільний пристрій для доступу до послуг і автентифікації.
Мобільний пристрій	Фізичний пристрій, такий як смартфон або планшет, який використовується користувачем для отримання та надсилання інформації про автентифікацію.
Мобільний додаток	Додаток, встановлений на мобільний пристрій користувача, який забезпечує взаємодію з системою MobileID.
SMS-шлюз	Серверна компонента, яка відправляє SMS-повідомлення на мобільний пристрій користувача для підтвердження автентифікації.
Серверна аплікація	Основна система, яка здійснює автентифікацію і управління даними користувачів.
Інтерфейси	API або інші інтерфейси, що забезпечують комунікацію між компонентами системи MobileID та іншими системами або додатками.
База даних	Зберігання і управління даними користувачів, налаштуваннями системи та журналами подій.

Принципи роботи системи MobileID містять [22]:

1) Мобільний пристрій як основний засіб автентифікації: У системі MobileID мобільний пристрій використовується як основний засіб для автентифікації користувача. Це означає, що користувач встановлює спеціальний додаток або програмне забезпечення MobileID на свій мобільний пристрій і використовує його для доступу до ресурсів або послуг, що потребують автентифікації, як проілюстровано на Рис.3.8.

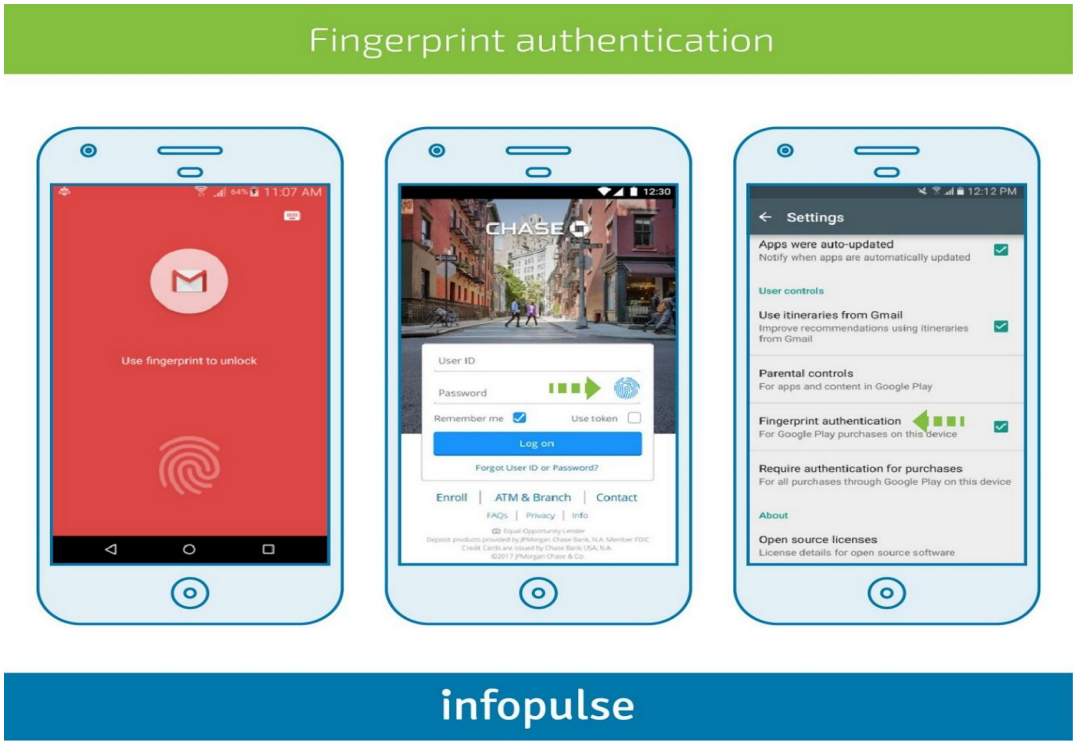

Рис.3.8.Використання системи автентифікації

2) Генерація та використання унікальних ідентифікаторів: При реєстрації в системі MobileID користувач отримує унікальний ідентифікатор, який пов'язаний з його мобільним пристроєм. Цей ідентифікатор використовується для ідентифікації користувача під час процесу автентифікації. Крім того, система MobileID може генерувати одноразові коди або токени, які також використовуються для підтвердження ідентичності користувача.

3) Захист даних та безпека комунікації: Система MobileID використовує різні механізми для захисту даних та забезпечення безпеки комунікації між клієнтом, сервером та ідентифікаційними серверами.

4) Багатофакторна аутентифікація: Система MobileID може підтримувати багатофакторну аутентифікацію, що означає використання декількох ідентифікаційних факторів для підтвердження ідентичності користувача. Приклади факторів,що можуть бути використані наведені в табл.3.5:

Табл.3.5. Фактори автентифікації, які підтримує система MobileID

Фактор автентифікації	Опис	Рівень безпеки	Використання у MobileID
Пароль	Секретний код, який вводиться користувачем	Середній	Так
Відбиток пальця	Біометричний шаблон відбитку пальця	Високий	Так
Обличчя	Біометричний шаблон обличчя	Високий	Так
Голос	Біометричний шаблон голосу	Високий	Так
Одноразовий код	Унікальний код, який генерується для кожного входу	Високий	Так
Апаратний ключ	Криптографічний ключ, що зберігається на пристрої	Високий	Так
SMS-підтвердження	Одноразовий код, який надсилається на мобільний пристрій	Середній	Так

5) Широке застосування в різних галузях: Система MobileID може бути застосована в різних галузях, включаючи фінансові установи, державні органи, електронну комерцію та багато інших сфер. Вона дозволяє забезпечити безпеку та зручність для користувачів при отриманні доступу до ресурсів та послуг, що потребують автентифікації.

Огляд системи автентифікації MobileID показує, що вона є зручним та безпечним рішенням для доступу до ресурсів та послуг через мобільні пристрої. Завдяки своїй архітектурі та принципам роботи, MobileID дозволяє користувачам з легкістю перевіряти свою ідентичність та отримувати доступ до необхідних ресурсів.

Використання та перспективи розвитку системи MobileID є значними і обіцяють багато переваг. Деякі з основних аспектів використання та перспектив розвитку MobileID включають:

1) Масове використання в сфері фінансів: MobileID має великий потенціал у фінансовій сфері, де безпека та автентифікація є критичними. Банки та фінансові установи можуть використовувати систему MobileID для

забезпечення безпеки операцій з клієнтами, включаючи виконання платежів, переказів коштів та доступ до банківських рахунків.

2) Розширення в електронній комерції: MobileID може стати важливим елементом в електронній комерції, дозволяючи здійснювати безпечні покупки та оплату товарів та послуг. Завдяки своїй безпеці та зручності, MobileID може замінити традиційні методи автентифікації, такі як введення пароля або використання банківських карток.

3) Застосування в державних органах: Урядові органи можуть використовувати систему MobileID для забезпечення безпеки та впровадження електронних послуг для громадян. Це може включати електронну ідентифікацію громадян, електронний доступ до публічної інформації, подачу електронних заявок та багато інших послуг.

4) Розвиток мобільних технологій: Зростаюча популярність мобільних пристроїв та швидкий розвиток мобільних технологій створюють сприятливе середовище для розвитку системи MobileID. Запровадження швидкого та безпечного способу автентифікації на основі мобільних пристроїв відкриває шлях до нових можливостей та додаткових функцій, що полегшують життя користувачів.

5) Розширення функціональності: У майбутньому система MobileID може розширити свою функціональність, включаючи біометричну автентифікацію, розпізнавання обличчя, використання голосового керування та інші інноваційні можливості. Це сприятиме ще більшій безпеці та зручності для користувачів.

Загалом, використання та перспективи розвитку системи MobileID обіцяють безпеку, зручність та розширення функціональності в різних галузях, що вимагають надійної автентифікації користувачів. Однак, необхідно враховувати аспекти приватності та безпеки даних при використанні таких систем та розвитку відповідних правових та технологічних механізмів для їх захисту.

Позитивні та негативні аспекти використання MobileID перераховані нижче в табл.3.6.

Незважаючи на ці недоліки, MobileID залишається зручним та ефективним інструментом автентифікації, особливо в контексті мобільних технологій та безпеки даних. При використанні правильних заходів безпеки та обережності, багато з цих негативних аспектів можуть бути зменшені або усунені, роблячи MobileID надійним рішенням для багатьох організацій та користувачів.

Табл.3.6. Плюси і мінуси використання MobileID

Позитивні аспекти	Негативні аспекти
Зручність та доступність	Залежність від мобільних пристроїв
Високий рівень безпеки	Потенційна загроза безпеки
Універсальність та масштабованість	Відсутність стандартизації
Зменшення ризику шахрайства	Потреба у доступі до мережі Інтернет
Мобільність	Вартість для користувачів

Загальний огляд системи автентифікації MobileID демонструє його значні переваги та потенціал, а також деякі обмеження, які потрібно враховувати. Архітектура MobileID базується на взаємодії між клієнтом, сервером MobileID та ідентифікаційними серверами. Цей процес забезпечує безпеку, надійність та зручність під час автентифікації. MobileID використовується для доступу до ресурсів, які вимагають автентифікації, і має перспективи розвитку в контексті росту мобільних технологій. Він забезпечує зручну та швидку автентифікацію з використанням мобільних пристроїв, що є все більш поширеним і популярним серед користувачів. Після аналізу плюсів та мінусів використання MobileID виявлено, що його переваги включають високий рівень безпеки, зручність, мобільність та широке застосування. Однак, існують і негативні аспекти, такі як залежність від мобільних пристроїв, потенційна загроза безпеки, відсутність стандартизації та потреба у доступі до мережі Інтернет. Враховуючи ці фактори, MobileID може бути ефективним рішенням для багатьох організацій та користувачів, якщо вжиті необхідні заходи безпеки та обережність. В подальшому розвитку системи MobileID варто звернути увагу на стандартизацію, покращення безпеки та розширення його застосування для забезпечення ще більшої зручності та надійності для користувачів.

3.3 Огляд системи автентифікації Державного інтернет-ресурсу "Дія"

Система автентифікації Державного інтернет-ресурсу "Дія" є ключовим компонентом електронного урядування, який дозволяє громадянам отримувати доступ до електронних послуг та ресурсів урядових органів. Загалом, система автентифікації Державного інтернет-ресурсу "Дія" забезпечує безпеку, зручність та доступність для користувачів, які мають можливість використовувати електронні послуги та ресурси урядових органів з високим рівнем довіри та автентичності. Архітектура та особливості роботи системи розроблені з урахуванням потреб користувачів та забезпечення вимог безпеки і конфіденційності [23].

Архітектура системи "Дія" включає наступні компоненти, наведені у табл.3.7:

Табл.3.7 Архітектура системи «Дія»

Складова	Опис
Клієнтський додаток	Мобільний додаток, який встановлюється на пристрої користувача та дозволяє отримувати доступ до послуг системи "Дія".
Сервери	Центральні сервери, що обробляють запити від клієнтських додатків та забезпечують роботу системи.
База даних	Сховище, де зберігаються дані користувачів, послуг та інша інформація, необхідна для функціонування системи.
API	Інтерфейс програмування додатків, який дозволяє здійснювати взаємодію з системою "Дія" через стандартизовані протоколи та методи.
Аутентифікація	Механізми для перевірки та підтвердження ідентичності користувачів, включаючи використання ЕЦП (електронного цифрового підпису).
Інтеграція	Можливість інтеграції системи "Дія" з іншими державними та комерційними сервісами для забезпечення широкого спектру послуг для користувачів.

Особливості роботи системи "Дія" охоплюють ряд аспектів, які забезпечують її ефективність та функціональність. Деякі з особливостей системи "Дія" включають:

1. Єдина точка входу: Система "Дія" надає єдину точку входу для користувачів, що дозволяє зручний доступ до різних державних ресурсів та послуг. Замість необхідності введення окремих ідентифікаційних даних для

кожного ресурсу, користувач може скористатися своїми обліковими даними "Дія" для автентифікації і отримання доступу.

2. Багатофакторна автентифікація: Система "Дія" підтримує багатофакторну автентифікацію, що означає використання кількох методів перевірки ідентичності користувача. Крім основних ідентифікаційних даних, таких як ім'я користувача та пароль, система може вимагати додаткові фактори, наприклад, одноразові паролі, біометричні дані або коди підтвердження, для забезпечення вищого рівня безпеки.

3. Інтеграція з державними системами: Система "Дія" інтегрована з різними державними системами та базами даних. Це дозволяє користувачам отримувати доступ до різних ресурсів, таких як електронні сервіси, документи, заяви та інші інформаційні послуги, шляхом автентифікації через систему "Дія".

4. Захист персональних даних: Система "Дія" має високий рівень захисту персональних даних користувачів. Вона використовує сучасні методи шифрування та захисту інформації, що забезпечує конфіденційність та недоступність даних третім особам.

5. Зручність та доступність: Система "Дія" надає зручний та простий інтерфейс для користувачів, що спрощує процес автентифікації та доступ до ресурсів. Користувачі можуть отримати доступ до різних послуг інтернет-ресурсів без необхідності повторного введення даних або запам'ятовування багатьох паролів.

Ці особливості сприяють забезпеченню зручності, безпеки та доступності при використанні системи "Дія" для автентифікації та отримання доступу до державних ресурсів та послуг.

Архітектура та особливості роботи системи "Дія" створюють базу для її ролі та використання в державних органах. Завдяки своїм особливостям, система "Дія" здатна впроваджуватися та використовуватися в різних сферах державного сектору з метою поліпшення якості та ефективності надання послуг громадянам. Деякі з ролей та використання системи "Дія" в державних органах включають:

1. Удосконалення електронних послуг: Система "Дія" може використовуватися для розширення доступу громадян до електронних послуг, наданих державними органами. Завдяки системі автентифікації "Дія", користувачі можуть отримати зручний та безпечний доступ до різних сервісів, таких як електронне звернення до влади, подання звітів та заяв, як на Рис.3.9, отримання електронних документів тощо.

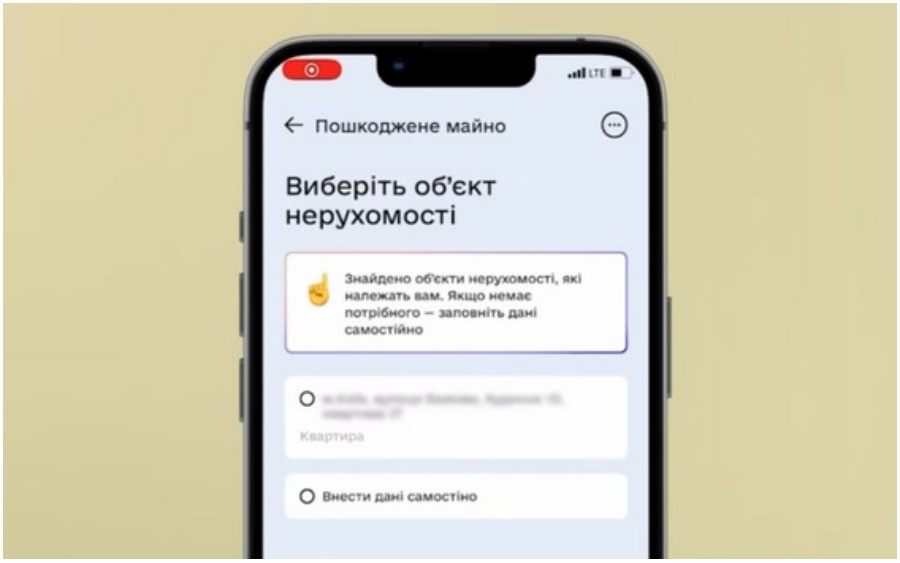

Рис.3.9. Приклад подачі зави

2. Спрощення бюрократичних процедур: Використання системи "Дія" дозволяє державним органам спростити та прискорити бюрократичні процедури. Завдяки автоматизованому доступу до інформації та забезпеченню безпеки даних, система "Дія" допомагає уникнути повторного збору та обробки інформації, забезпечуючи швидше та ефективніше надання послуг громадянам.

3. Інтеграція з існуючими системами: Система "Дія" може бути інтегрована з існуючими інформаційними системами державних органів. Це дозволяє обмінюватися даними між різними системами та забезпечувати єдиний доступ до інформації. Наприклад, система "Дія" може інтегруватися з системою податкової служби, медичною системою, системою соціального захисту тощо, що дозволяє державним органам ефективніше обмінюватися та використовувати інформацію.

4. Забезпечення безпеки та конфіденційності: Система "Дія" має високі стандарти безпеки, що є важливим аспектом для державних органів. Вона забезпечує захист персональних даних громадян, аутентифікацію користувачів та контроль доступу до ресурсів. Це сприяє забезпеченню конфіденційності та захисту інформації при обробці державних даних.

Загалом, система "Дія" використовується в державних органах для поліпшення доступу громадян до електронних послуг, спрощення бюрократичних процедур, інтеграції з іншими системами та забезпечення безпеки та конфіденційності даних. Це допомагає державним органам покращувати якість та ефективність надання послуг громадянам у цифровому середовищі.

Оцінка ефективності та безпеки системи ДІЯ є важливим аспектом для державних органів, які використовують цю систему. При оцінці ефективності системи ДІЯ враховуються такі фактори:

1. Швидкість та доступність: Система ДІЯ повинна забезпечувати швидкий та безперебійний доступ до електронних послуг для користувачів. Це означає, що система повинна працювати ефективно, оптимізувати час відповіді та мати високу доступність, щоб користувачі могли без затримок отримувати необхідні послуги.

2. Надійність та стабільність: Система ДІЯ повинна бути надійною та стабільною. Це означає, що вона повинна працювати без відмов та відновлюватися швидко у разі виникнення неполадок або відмов. Надійність системи є важливою для забезпечення безперебійного надання послуг громадянам та підтримки роботи державних органів.

3. Масштабованість: Система ДІЯ повинна бути масштабованою, щоб відповідати зростаючим потребам користувачів. Завдяки гнучкій архітектурі та інфраструктурі, система повинна бути здатною швидко масштабуватися, коли з'являється більше користувачів або збільшується обсяг оброблюваної інформації.

4. Забезпечення конфіденційності та безпеки: Система ДІЯ повинна гарантувати високий рівень конфіденційності та безпеки даних користувачів. Це означає, що система повинна мати захист від несанкціонованого доступу, шифрування комунікацій та застосування надійних методів автентифікації. Забезпечення безпеки є критичним аспектом, оскільки система містить чутливу інформацію про користувачів та державні послуги.

У процесі оцінки безпеки системи ДІЯ враховуються наступні аспекти:

1) Вразливості та ризики: Проводиться аналіз вразливостей системи, ідентифікуються потенційні ризики, які можуть виникнути при використанні системи. Це допомагає виявити можливі проблеми та прийняти заходи для їх запобігання або зменшення наслідків.

2) Заходи безпеки: Оцінюються заходи безпеки, які впроваджені в системі. Це включає методи аутентифікації, шифрування даних, контроль доступу та інші заходи для захисту інформації.

3) Система моніторингу та реагування: Перевіряється, чи наявні системи моніторингу та реагування на можливі інциденти безпеки. Це допомагає вчасно виявляти аномалії, вторгнення або неправомірну діяльність та приймати необхідні заходи для реагування.

4) Політики безпеки: Оцінюються політики безпеки, що встановлені для використання системи ДІЯ. Це включає правила та процедури, які дотримуються для забезпечення безпеки, а також надання доступу та обробки даних.

Оцінка ефективності та безпеки системи ДІЯ допомагає державним органам переконатися, що система відповідає їх вимогам щодо швидкості, доступності, безпеки та конфіденційності. Це сприяє покращенню якості надання державних послуг громадянам та забезпеченню довіри до системи ДІЯ.

ВИСНОВКИ

З аналізу принципів технології делегованої автентифікації встановлені основні її переваги (спрощення процесів для користувачів, підсилення безпеки та зниження навантаження на інформаційну систему, розширення функціональності та інтеграції) та недоліки (обов’язковий доступ до телекомунікаційних мереж, залежність від провайдерів, вартість інтеграції і підтримки тощо). Зазначено, що для успішного розвитку систем делегованої автентифікації необхідними є стандартизація та інтеграція наявних протоколів і стандартів, що забезпечить сумісність та інтероперабельність між різними системами та спростить процес подальшого впровадження технології.

Проведений аналіз архітектур присутніх в Україні систем делегованої автентифікації (BankID, MobileID та системи ДІЯ) дозволяє зробити оптимальний вибір зручного та безпечного способу перевірки особистості користувача у залежності від сценарію надання йому певних цифрових послуг.

СПИСОК ВИКОРАСТАННИХ ДЖЕРЕЛ

1. Shehab M. A., & Al-Yaseen W. A comprehensive survey on single sign-on authentication and its security. Computers & Security. 2017.
2. Jones M., Bradley J., Sakimura N. OAuth 2.0: An Overview and Introduction to the OAuth 2.0 Standard. 2015.
3. What Delegated Authentication Is & How It Works - JumpCloud. *JumpCloud*. URL: https://jumpcloud.com/blog/what-is-delegated-authentication
4. Hardt D. The OAuth 2.0 Authorization Framework. 2012.
5. Li W., Mitchell J. C. "Delegation Logic: A Logic-Based Approach to Secure Authorization in Open Systems". 2005.
6. Розробка веб-сервісів і мобільних додатків | компанія stfalcon.com. *Custom Software Development Company | Stfalcon.com*. URL: https://stfalcon.com/uk (дата звернення: 22.06.2023).
7. OpenID Connect (OIDC). *Identity Security for the Digital Enterprise | Ping Identity*. URL: https://www.pingidentity.com/en/resources/identity-fundamentals/authentication-authorization-standards/openid-connect.html#:~:text=OpenID%20Connect%20(OIDC)%20is%20an,network,%20to%20authenticate%20their%20identities.
8. web_page_person. What is SAML ? Security Assertion markup Language - TutorialKart. *TutorialKart*. URL: https://www.tutorialkart.com/salesforce/what-is-saml-security-assertion-markup-language/#gsc.tab=0
9. [MS-KILE]: Kerberos Network Authentication Service (V5) Synopsis. *Microsoft Learn: Build skills that open doors in your career*. URL: https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-kile/b4af186e-b2ff-43f9-b18e-eedb366abf13
10. What is SSL/TLS Encryption?. *F5 | Multi-Cloud Security and Application Delivery*. URL: https://www.f5.com/glossary/ssl-tls-encryption
11. What is FIDO (fast identity online)? Meaning from wallarm. *End-to-end API Security for Cloud-Native Applications âšœ①ï¸ ❹ - Wallarm*. URL: https://www.wallarm.com/what/what-is-fido-fast-identity-online
12. Gramila J. Building a WebAuthn Application with Java. *Okta Developer*. URL: https://developer.okta.com/blog/2022/04/26/webauthn-java
13. Shibboleth consortium - shaping the future of shibboleth software. *Shibboleth Consortium*. URL: https://www.shibboleth.net/
14. What is active directory federation services (ADFS)? - jumpcloud. *JumpCloud*. URL: https://jumpcloud.com/blog/what-is-adfs

15. Qasim S. M., Kim H. J."A Comparative Study on Security Analysis of Delegated Authentication in Mobile Health Systems". 2019.
16. Pay with biometric is not as convinient as you think | WIRED Middle East. WIRED Middle East. URL: https://wired.me/technology/pay-with-your-biometric-palm-face-fingers-whats-next/
17. Park J., Park J. "Delegated Authentication Method for Financial Services using OpenID Connect". 2019.
18. BankID. *Curity Identity Server Docs*. URL: https://curity.io/docs/idsvr/latest/authentication-service-admin-guide/authenticators/bankid.html
19. Implementing BankID in a merchant application - Kiev-Open (COI). *Dashboard - Confluence*. URL: https://confluence.bankidnorge.no/confluence/kiev-open/bankid-implementation-guide/implementing-bankid-in-a-merchant-application
20. Mobile ID | Identification for Development. *Home | Identification for Development*. URL: https://id4d.worldbank.org/guide/mobile-id
21. Frequently asked questions. *Sicher online einloggen mit Mobile ID*. URL: https://www.mobileid.ch/en/faq
22. Дія – Державні послуги онлайн. *Державні послуги онлайн | Дія*. URL: https://diia.gov.ua/
23. Українська правда. Застосунок “Дія”: захист персональних даних і безпека. *Українська правда*. URL: https://www.pravda.com.ua/columns/2020/02/8/7239861/