Аналітичний огляд
Архітектура та безпека електронного уряду в ЄС

к.ф.-м.н. Мартиненко С.В.

Анотація

Ця публікація має на меті проаналізувати стан речей в галузі електронного уряду (e-government, Е-Уряд) та захисту громадян щодо обробки їх персональних даних в Євросоюзі, та на основі такого аналізу сформулювати першочергові задачі для розбудови Е-Уряду в Україні.

Наводиться перелік впроваджених послуг Е-Уряду в ЄС, розглядаються питання архітектури Е-Уряду та питання забезпечення безпеки доступу до послуг системи Е-Уряд з використанням Національної системи персональних ідентифікаторів, електронних підписів тощо.

1. Вступ

1.1. Терміни

Робоча група захисту даних (Data protection working party) - Робоча Група була заснована Статтею 29 Директиви 95/46/ЕС. Це - незалежний Консультативний Орган ЄС по Захисту Даних та Конфіденційності. Його задачі встановлені в Статті 30 Директиви 95/46/ЕС та в Статті 14 Директиви 97/66/ЕС.

Європейське агентство мережевої та інформаційної безпеки (ENISA - European Network and Information Security Agency). Його головні задачі - забезпечити допомогу і надати рекомендації Комісії ЄС та Державам–членам щодо проблем, пов'язаних з мережевою та інформаційною безпекою для того, щоб гарантувати безперешкодне функціонування внутрішнього ринку. Це допоможе досягти збільшення координації та інформаційного обміну між зацікавленими сторонами по інформаційній безпеці. Агентство призвано забезпечити механізм розвитку культури безпеки.

1.2. Стан розвитку послуг електронного уряду в ЄС

Розвиток електронного уряду складає сьогодні в більшості Держав-членів ЄС одну з пріоритетних задач діяльності в межах їх політик модернізації державних органів. Такий пріоритет на європейському рівні виражається ухваленням Європейською Радою Feira в червні 2000 «Плану дій e-Europe 2002», який включає розділ «он-лайн уряд» (т.б. електронний або інтерактивний уряд). Нині спостерігається розвиток різних проектів Е-Уряду. В більшості з цих проектів звертається увага до проблеми комплексного захисту даних для того, щоб гарантувати успіх проектів Е-Уряду.

Робочий документ по Е-Уряду (10593/02/EN WP 73 від 8 травня 2003 р., Робоча група захисту даних) зазначає перелік впроваджених послуг Е-Уряду в ЄС, зокрема:

1. У першу чергу, ряд країн надали громадянам можливість за допомогою інтерактивних процедур подати декларації про прибутки/податки з можливістю інтерактивної оплати, а також послуги з надання консультацій по файлу особи. Сектор державних фінансів (бюджету) поза сумнівом складає привілейовану область Е-Уряду.
2. Сповіщення державних органів про зміну адреси. Оскільки таке сповіщення складає звичайну (і навіть обов'язкову), після податків, адміністративну формальність у багатьох країнах, то це інтерактивна адміністративна процедура, яка найбільш часто реалізується. Ці послуги застосовують різний рівень безпеки (в залежності від країни), деякі з них (Іспанія, Фінляндія, ін.) реалізують за допомогою системи електронного підпису.
3. Наступна поширена інтерактивна процедура - це науково-дослідні роботи.

4. Список інших інтерактивних процедур, які реалізуються в Е-Уряді:
- запит ліцензії на будівництво,
- тимчасове користування виданнями в публічних бібліотеках,
- запити на документи від Загсу (бюро запису актів громадянського стану),
- реєстраційні процедури для нових компаній,
- соціальні податки,
- відносини з професіоналами/ фахівцями оздоровчих установ,
- реєстрація в школах і університетах,
- реєстрація для іспитів,
- реєстрація автомобіля,
- компенсація медичних витрат,
- реєстрація скарг (поліція, судочинство).

На сучасному етапі розвитком програми Е-Уряду в ЄС є такі програми: «Електронна митниця» (eCustoms), «Електронний паспорт» (ePassport), «Електронне голосування» (eVoting).

2. Архітектура послуг електронного уряду

2.1. Архітектура Е-Уряду

Майже всі країни ЄС застосували для побудови «портальний» підхід, тобто розвиток унікальної/ єдиної точки входу до інтерактивних державних процедур. Ця загальна тенденція з'являється в країнах, де вже були розроблені вузли (сайти), які більш-менш відігравали роль незалежних порталів, а також країнах, де до цього не існувало ніякої системи.

У деяких випадках, за цей портал відповідальним є специфічне міністерство. Так, у Фінляндії, вузол http://www.suomi.fi управляється Міністерством Фінансів; в Австрії портал Федерального Уряду http://www.help.gov.at також управляється Міністерством Фінансів.

Ці портали загалом призначаються як сайти загальної інформації, які містять: посилання на різні державні та інституційні (відомчі) послуги; адреси адміністрацій і державних установ; інформаційні файли; цитати з Офіційного Журналу (ЄС) щодо різних процедур (форми; інформація щодо адміністративних процедур; інформація щодо фінансової допомоги, запити на фундації, пропозиції робочих місць в державному секторі тощо); інформація щодо національного законодавства; поточні події; блок пропозицій; публікації і т.д.

Все частіше ці портали також використовуються, щоб отримати доступ до адміністративних процедур, які стосуються як громадян так і компаній (бізнесу). Тому виникає проблема можливості збереження особистих даних на порталі. На даний час ці вузли не зберігають особистих даних в Данії, Німеччині, Іспанії, Португалії та Швеції. Проте, такі вузли можуть або будуть здатні зберігати особисті дані в Бельгії, Італії, Норвегії, Фінляндії, Австрії (виключно, якщо громадянин звертається до процедури, яка вимагає ототожнення/ аутентифікації) і Ірландії.

Наприклад, в Ірландії система забезпечує можливість інтерактивної (on-line) реєстрації. Реєстрація складається з аутентифікації (підтвердження) ідентичності за допомогою Персонального Номера Державної Послуги (PPSN, person's Public Service Number) і надання державних служб через Брокера, який утримує особисті дані в безпечному центральному сховищі даних. Ідентичність персони засвідчується Базою даних Ідентичності Державного Сервісу (Public Service Identity Database), яка містить основні деталі ідентичності та управляється Департаментом Соціальних та Сімейних Справ (Department of Social and Family Affairs). Система забезпечує додаткові вимоги аутентифікації для більш

безпечних і конфіденційних операцій/ транзакцій.

Доступ до послуг через Брокера заснований на індивідуальній згоді суб'єкта - не вимагається обов'язковість використання системи громадянином. Особисті дані (наприклад, дата народження, паспортні дані, прибутки/ доходи, сімейні взаємозв'язки і т.д) зберігаються Брокером в центральному сховищі даних. Брокер управляє цією інформацією та захищає її. Доречні дані надаються через Брокера в ході трансакції тільки агентству державної послуги відповідно до спеціальних інструкцій користувача. Розробляються відповідні політики безпеки для різних послуг, особисті дані в сховищі шифруються. Після остаточного закінчення розробки системи Брокер матиме можливість передбачати життєві події (наприклад, пенсія); і кожна категорія системи матиме «інтелект», щоб запропонувати доцільні для персони покажчики/ дані/ послуги. Отже, Брокер через портал забезпечить для персон «Інтернет магазин» (one-stop shop) послуг державних служб/ сервісів.

2.2. Виконання послуг Е-Уряду з залученням комерційних компаній

Зв'язок між електронним урядом і комерційним сектором може виражатися також в тому, що робота адміністративних процедур забезпечується приватними (не державними) акціонерними компаніями. Це примушує розглядати різні аспекти щодо організації електронних державних служб. Наприклад, як можуть приватні акціонерні компанії гарантувати рівноправність в процедурах обробки; як вони (послуги) оплачуються; чи мається на увазі, що адміністративні процедури не повинні бути вільно доступними і т.д?

Через зазначені проблеми, в Німеччині, Італії, Іспанії, Нідерландах, Швеції та в Норвегії було вирішено не звертатися до приватних постачальників послуг, які б могли мати доступ до персональних даних користувачів. Проте в більшості країн ЄС, і більш всього в Іспанії, органи державної влади звертаються до послуг приватних зовнішніх постачальників, наприклад, з метою розробки та розвитку порталу. В Іспанії, до того ж, приватні оператори також залучаються до виконання аудиту щодо планування розробки порталів.

Протилежний вибір зроблено в Бельгії, Данії, Франції (тільки частково), Фінляндії та Австрії, де будь-який приватний постачальник може звернутися за офіційним визнанням (отриманням дозволу) після того як довів, що він здійснюватиме необхідні гарантії безпеки, особливо щодо захисту даних. В Португалії та Англії не існує із цього приводу ніяких формальних обмежень, там не має ніяких принципових заперечень щодо факту залучення приватних зовнішніх постачальників послуг.

Вимоги до приватних зовнішніх постачальників послуг в окремих державах містять такі гарантії: відповідний контракт з процесорами даних; точне визначення місій зовнішніх приватних постачальників; визначення вимог безпеки (захищене та повністю автоматизоване оточення); відповідність приватних зовнішніх постачальників специфічним законодавчим вимогам (акредитація), що включають зокрема заборону використовувати дані для інших цілей, ніж ті, для яких вони були зібрані, або заборону розголошувати ці дані; точне визначення даних, які реєструються; можливе створення/ визначення комітетів/ комісій з інспекції, і т.п.

3. Безпека послуг електронного уряду

3.1. Проблеми безпеки

Мережева та інформаційна безпека є передумовою інформаційного суспільства, як визначено в Повідомленні Комісії для Ради та парламенту Європи (Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - eEurope 2005 Mid-term Review, COM/2004/0108 final). Зазначається, що майже 80% європейських громадян не користуються закупками в Інтернеті через побоювання безпеки. Деякі Держави-члени розробляють національні стратегії по інформаційній безпеці, законодавчі зобов'язання та відповідальність, заходи збільшення правосвідомості, затверджують перелік технічних стандартів тощо.

Високий пріоритет щодо питань безпеки на рівні ЄС витікає із створення Європейського агентства мережевої та інформаційної безпеки (ENISA - European Network and Information Security Agency).

Проблемами безпеки, які розглядаються, зокрема є:

- Досягнення більш широкого прийняття ринком електронних підписів (e-signatures) за допомогою просування на європейському рівні використання міждіючих (interoperable) стандартів і просування всіх форм електронних підписів;
- Роль стандартів та сертифікації в створенні довіри в інформаційному суспільстві;
- Ідентифікація пріоритетів для кооперації на рівні ЄС у сфері мереженої та інформаційної безпеки, зокрема в структурі ENISA (розвиток співпраці на рівні ЄС, інвентаризація діяльності та організацій Держав-членів, кращі методи у сфері збільшення правосвідомості та оцінки ризиків тощо).

Робочий документ по Е-Уряду (10593/02/EN WP 73 від 8 травня 2003 р.) зазначає, що за винятком Бельгії та Німеччини, всі уповноважені захисту даних (Data Protection Authorities) консультувалися [*з Робочою групою захисту даних ЄС*] щодо проектів інтерактивних державних процедур, що здійснювалися в їх країні.

3.2. Національні системи персональних ідентифікаторів

Розглядаються два типи ідентифікаторів особи (персональних ідентифікаторів) – ***унікальні загальні*** (єдиний ідентифікатор на національному рівні) та ***секторні*** (громадянин може мати ряд ідентифікаторів, кожен з яких застосовується в своєму «секторі», наприклад, ідентифікатор платника податків, ідентифікатор соціального страхування тощо).

Країни, що впровадили *унікальну державну ідентифікацію* на національному рівні, - це Бельгія, Данія, Іспанія, Фінляндія, Ірландія, Італія, Люксембург, Норвегія та Швеція. Проекти розвитку таких унікальних ідентифікаторів існують в інших країнах, зокрема в Австрії, але тільки як приховане початкове число (номер) для заснованих на секторних ідентифікаційних чисел (sector-based identification numbers) (див. нижче). В Данії, Бельгії і Іспанії, цей унікальний ідентифікатор співіснує із секторними ідентифікаторами. В країнах, що залишаються, існують тільки секторні ідентифікатори: Німеччина (соціальне страхування, номер паспорта), Франція і Португалія (по суті номер соціального страхування), Греція, Нідерланди (зокрема, державний податковий ідентифікатор). Треба зазначити, що в країнах подібно Німеччині і Португалії, використання унікального ідентифікатора розглядається як неконституційне.

Розвиток Е_Уряду іноді створює причини перегляду існуючої системи ідентифікаторів або розширення діапазону секторних ідентифікаторів. В даний час, тільки в Португалії та в Австрії розвиток Е-Уряду привів до ревізії їх національної системи ідентифікації громадян.

Загальною тенденцією для доступу до інтерактивних адміністративних процедур є використання наперед встановлених (існуючих) ідентифікаторів або унікальних (Бельгія, Данія, Іспанія, Ірландія), або секторних (Франція, Нідерланди, Португалія, Італія). В деяких країнах, де не існували унікальні ідентифікатори, підтвердилося, що реалізація персоналізованого порталу адміністрації не вимагає обов'язково створювати такий унікальний ідентифікатор (Франція, зокрема). Австрія становить специфічний випадок в цьому відношенні, оскільки для цього було створено унікальне ідентифікаційне число (число Реєстру Резидентів - Residents' Register number), яке не повинне зберігатися поза межами Реєстру Резидентів, і використовується тільки як секторні ідентифікатори за допомогою спеціально захищеної процедури. Ніякому органу державної влади не дозволяється зберігати ідентифікаційні секторні числа поза межами Реєстру.

Проекти використання секторних ідентифікаторів для доступу до інтерактивних адміністративних процедур були, або все ще розглядаються в певних країнах. Так, проект генералізації державного податкового ідентифікатора (social-fiscal identifier) в Нідерландах не був реалізований (відступив) через негативні думки з цього приводу. В даний час, такий проект існує тільки в Італії, де податковий ідентифікатор (платника податку) генералізується, щоб отримати унікальний ідентифікатор доступ до певних інтерактивних адміністративних процедур. В Ірландії, PPSN ("Персональне Число Державного Сервісу") передбачене законом як унікальне ім'я доступу до державних послуг і, згідно з законодавством, може використовуватися для податкових і державних послуг, а також інших послуг органів державної влади.

З метою ліквідації ризиків взаємного зв'язку, інші ограни заявляють, що повинен використовуватися один секторний ідентифікатор, зокрема в Нідерландах, де попередній проект уряду саме був тому змінений, та в Австрії, де (приховане) унікальне ідентифікаційне число, поєднане з електронним підписом в спеціальній функції (так звана «Burgerkarte» або «Цивільна Карта» - «Citizen Card»), використовуватиметься для забезпечення інтерактивного доступу до всіх інтерактивних додатків Е-Уряду, і навіть спеціально структурованих в приватному секторі.

У Бельгії, розвиток Е-Уряду дав шанс створити унікальне ім'я для бізнес-структур: Поточне VAT-номер (розширений до компаній та організацій, які не є членами VAT) перетворено на унікальний ідентифікатор для всіх бізнес-структур і організацій; цей номер замінює всі інші специфічні номери (числа) та вводиться як унікальне ім'я (ідентифікатор) для компаній та організацій для всіх інформаційних систем Е-Уряду.

3.3. Захист персональних даних

Окремою турбота розвитку Е-Уряду є питання, яке яскраво виражене англійськими повноважними органами, - це те, що розвиток Е-Уряду не повинен діяти, як «димова завіса» (smokescreen) прихованої генералізації державних інформаційних баз даних і збільшеного обміну особистими даними між державними органами (адміністраціями). Загальною доктриною повинна бути відмова від будь-якого взаємного передавання (обміну) файлами (даними про особу), Е-Уряд не повинен приводити до зростання рівня контролю за індивідуумами, контролю, що походить в першу чергу від об’єднання даних.

Треба підкреслити, що в Німеччині цю проблему (об’єднання даних) розглядав німецький Верховний Суд та затвердив його знамениту теорію «право на інформаційне самовизначення» індивідуумів. Це право полягає в тому, що кожен індивідуум має право вирішити щодо передавання та використання його/її даних третіми сторонами. Визнання цього права, яке не дорівнює абсолютній забороні комунікацій, як мінімум, обмежує багато можливостей комунікацій.

Зазначена проблема вимагає законодавчого вирішення. Так, в Англії було прийнято Королівський Декрет (Royal Decree) від 28 лютого 2003 щодо регулювання/ регламенту телематік-реєстрів (записів дистанційної обробки даних). Цей Декрет також встановлює процедури, які повинні використовуватися, щоб застосовувати ці системи, зокрема в контексті комунікацій з громадянами або для обміну інформацією в межах державних відомств. В останньому випадку, потрібна попередня згода суб’єкта даних. Декрет містить також статтю, яка вимагає обов'язкового дотримання державними адміністраціями Закону про захист даних (Data Protection Act).

Таким чином, важливо встановити баланс між взаємним обміном даними (що передбачає поліпшення державних послуг) та захистом користувачів щодо обробки їх персональних даних. Для пошуку цього балансу обов'язково необхідно виконати такі кроки аналізу:

- якими є очікувані переваги використання даних і їх взаємного обміну щодо задач Е-Уряду;
- чи є будь-які альтернативні підходи, щоб досягти тієї ж мети;
- якими є ризики та витрати, пов'язані з взаємним обміном даними;
- що може бути необхідними гарантіями, щоб управляти цими ризиками;
- завершення аналізу, - баланс між вигодами та ризиками, що пов'язані з взаємним обміном даними.

В той же час, необхідно підкреслити, що взаємний обмін даними між державними адміністраціями не є неминучим, щоб поліпшити послуги адміністрації – можливі інші рішення.

3.4. Електронний підпис та інфраструктура відкритих ключів (PKI)

У більшості Держав-членів є, або дозволяється, участь приватних операторів, «постачальників послуг видачі сертифікатів» (Центрів сертифікації), в межах реалізації для певних інтерактивних адміністративних процедур електронних механізмів підпису. В цих випадках, Центру сертифікації надається відповідний статус (наприклад, укладенням угоди). Ці проблеми у більшості були врегульовані під час приведення у відповідність національного законодавства до Директиви про електронні підписи.

У деяких випадках, що мають місце, послуги приватних постачальників не допускаються внаслідок факту, що тільки Держава гарантує цю роль (Німеччина, Іспанія). У Франції, ця роль діє за умовчанням: дотепер приватні зовнішні постачальники діють тільки в контексті видачі сертифікатів для VAT (податок на додану вартість - Value Added Tax) декларацій; у всіх інших випадках, Держава грає роль Центру сертифікації ключів.

Впровадження PKI ще не завершено в багатьох Державах-членах. Тому певних адміністративних процедур також немає, тому що вони вимагали б реалізації засобів електронного підпису та шифрування. За певним винятком, багато державних адміністрацій все ще не мають державних процедур, які б пов'язувалися з механізмом електронного підпису. Один з таких винятків - це Данія, де механізми електронного підпису вже розроблені. Тому електронні підписи для громадян роздані безкоштовно та багато Інтернет порталів можуть надати послуги Е-Уряду. Інші винятки наведені в Частині 2 Аналітичного огляду («Сучасні програми розвитку Е-Уряду»).

Області додатків, які використовують PKI, мають різні пріоритети в різних країнах, наприклад, сектор оподаткування та соціальний сектор у Франції, реєстрація населення у Фінляндії. В більшості випадків, механізми PKI однаково стосуються індивідуумів, компаній та державних агентств. Іноді першими користувачами PKI є індивідууми (Німеччина); іноді працівники організацій та сервери, і тому не переважно індивідууми (Данія), іноді державні агентства є першими щодо використання засобів PKI (Норвегія). В Норвегії, наприклад, електронні підписи представників влади не стільки вимагаються для ідентифікації індивідуума за його підписом, скільки для ідентифікації чи має персона, яка підписалася, необхідні повноваження ухвалити рішення або здійснити певну дію (т.б. ідентифікація повноважень).

Загальне відношення до механізмів електронного підпису позитивне, так як вони механізми як механізми, які придатні для підтримання захисту персональних даних.

4. Роль стандартизації в ЄС

Питанню стандартизації в ЄС приділяється надзвичайна увага. Стандартизація є складовою частиною політики Ради та Комісії ЄС з метою реалізувати «краще регулювання», збільшення конкурентноздатності підприємств та виключити бар'єри в торгівлі на міжнародному рівні. Це було підтверджено Резолюцією Європейським Парламентом в 1999 (Resolution on the report from the Commission to the Council and the

European Parliament “Efficiency and Accountability in European standardisation under the New Approach”, OJ C 150 of 28.5.1999) та Радою ЄС в її Резолюції від 28 жовтня 1999 (Council Resolution of 28 October 1999 on "the Role of Standardisation in Europe", OJ C141 of 2000 05-19), а також висновками від 1 березня 2002 року щодо ролі стандартизації в Європі (Council conclusions on standardisation of 2002-03-01, OJ C66 of 2002-03-15).

Висновки розглядалися в Повідомленні від Комісії до Європейського Парламенту та Ради від 18.10.2004 (COM(2004) 674 final, Communication from the Comission to the European Parliament and the Council **on the role of European standardisation in the framework of European policies and legislation,** SEC(2004) 1251). Головним висновком є те, що політика з питань стандартизації в Європі є успішним інструментом для створення Єдиного Ринку.

Керуючись цим висновком, архітектура системи Е-Уряду бути стандартизована та включати Рамкову структуру архітектури інформаційних технологій, Технічну еталонну модель (Technical Reference Model) та Профіль стандартів, в тому числі Профіль стандартів безпеки (Security Standards Profile). Розроблено також відповідні стандарти обміну інформацією між державними службами на міждержавному рівні Держав-членів. Повинні також бути визначені технічні стандарти взаємодії між державними службами в межах держави та між державною службою і користувачами (громадянами та бізнесом).

5. Висновки

Виходячи з досвіду країн ЄС, для розбудови Е-Уряду в Україні необхідно виконати такі заходи:

1. ***Розробити національну стратегію розбудови Е-Уряду*** в Україні. Визначити в ній перелік інтерактивних процедур, які повинні бути реалізовані в межах задач Е-Уряду. Перелік може (й повинен) включати послуги різних міністерств та відомств з визначення черговості впровадження. За основу можна взяти перелік послуг, наведений в п. 1.2. цього огляду.
2. ***Розробити національну стратегію по інформаційній безпеці Е-Уряду***, визначивши законодавчі зобов'язання та відповідальність, заходи збільшення правосвідомості, національну систему(и) персональних ідентифікаторів для послуг Е-Уряду тощо.
3. ***Затвердити перелік технічних стандартів Е-Уряду***. Будь-яка архітектура системи повинна включати Рамкову структуру архітектури інформаційних технологій, Технічну еталонну модель (Technical Reference Model) та Профіль стандартів (в тому числі Профіль стандартів безпеки - Security Standards Profile). В найбільш передових системах розробляються також відповідні стандарти обміну інформацією між державними службами та між державною службою та користувачем (громадянами та бізнесом).
4. ***Привести у відповідність законодавство України щодо електронного підпису, закріпити законодавче «право на інформаційне самовизначення» громадян***, привести законодавство України у відповідність до законодавства ЄС щодо: а) захисту персональних даних; б) щодо електронних підписів; б) електронної комерції; с) електронних банківських операцій.