Рекомендації для підготовки документів міжнародної платіжної системи, платіжною організацією якої є нерезидент, що подаються до Національного банку України, в частині захисту інформації

1. Загальні положення

Ці Рекомендації розроблено на підставі вимог Положення про порядок реєстрації платіжних систем, учасників платіжних систем та операторів послуг платіжної інфраструктури, затвердженого постановою Правління Національного банку України від 04.02.2014 № 43 (далі – Положення № 43).

Метою Рекомендацій є надання допомоги міжнародним платіжним системам, платіжною організацією яких є нерезидент, під час підготовки документів для узгодження умов та порядку діяльності в Україні міжнародних платіжних систем (далі – МПС) в частині захисту інформації.

Відповідно до вимог розділу IV Положення № 43 для узгодження умов та порядку діяльності в Україні міжнародної платіжної системи (далі – Документи МПС) платіжна організація повинна подати до Національного банку технологію обміну інформацією в міжнародній платіжній системі та опис системи захисту інформації, яка використовуватиметься МПС на території України.

Якщо Документи МПС включають відомості щодо захисту інформації, які містять банківську таємницю, то такі відомості мають бути викладені в окремому документі, оформленому відповідно до нормативно-правових актів Національного банку України.

Терміни та поняття, які вживаються в Рекомендаціях, застосовуються в значеннях, визначених законами України та нормативно-правовими актами Національного банку України.

2. Схема та опис руху інформаційних повідомлень

Рекомендуємо, що Документи МПС мають містити схему руху інформаційних повідомлень (далі – Схема обміну), яка може бути суміщена з іншими схемами, наприклад, зі схемою руху коштів. Оскільки не всі інформаційні повідомлення містять інформацію про платежі, у розділі, що описує систему захисту інформації платіжної системи, рекомендовано надати спеціалізовану схему руху інформаційних повідомлень, яка містить тільки ті компоненти системи, що приймають участь в обміні та обробленні такої інформації. Ця рекомендація не є обов’язковою і в описі системи захисту можна посилатись на загальну Схему обміну.

Схема обміну має містити всі компоненти платіжної системи, які функціонують в системі. Такими компонентами можуть бути: учасники МПС, платники та отримувачі коштів, оператори послуг платіжної інфраструктури,

розрахунковий банк, процесинговий центр, надавачі електронних довірчих послуг, програмно-технічні комплекси генерації та сертифікації ключів, інші компоненти для забезпечення функціонування міжнародної платіжної системи в Україні. Якщо учасник – резидент МПС (далі – учасник) має в своєму складі декілька компонент (наприклад, робоче місце касира та віддалений сервер, з яким він зв'язується по мережі), вони мають бути відображені на Схемі обміну окремо.

На Схемі обміну рекомендовано показати взаємодію між клієнтами (платники та отримувачі коштів) та учасниками або компонентами МПС, якщо така взаємодія можлива різними способами (наприклад, через Інтернет-сайт та за допомогою програмно-технічного комплексу самообслуговування).

Рекомендовано всі компоненти схеми, між якими передається інформація про платіж, дані платників та отримувачів, а також криптографічні ключі, з'єднувати за допомогою пронумерованих стрілок.

У випадку, якщо учасник – резидент МПС обмінюється платіжною чи ключовою інформацією з іншими платіжними системами, ці платіжні системи також мають бути показані на Схемі обміну разом з ланками обміну інформацією.

В Документах МПС рекомендуємо надати опис технічного та криптографічного захисту для кожної ланки Схеми обміну з посиланням на номер ланки.

3. Надання копій дозвільних документів на використання засобів захисту

Для засобів технічного та криптографічного захисту інформації, які використовуються чи будуть використовуватись учасниками – резидентами в міжнародній платіжній системі, необхідно надати копії чинних експертних висновків уповноваженого органу. Це може бути Державна служба спеціального зв'язку та захисту інформації України (далі – Держспецзв'язок) або авторитетні міжнародні організації, що сертифікують такі засоби, наприклад, NIST.

Вказані експертні висновки мають бути чинними на момент подання Документів МПС до Національного банку України. Для засобів технічного захисту інформації допускається чинність на момент придбання засобу.

4. Опис засобів захисту мережі

В якості технічного захисту мереж, що забезпечують взаємодію учасників – резидентів між собою та з компонентами системи, які розміщені поза межами України, можуть використовуватись програмні та програмно-апаратні засоби захисту мережі. В описі Схеми обміну рекомендуємо вказати

вимоги, які висуває міжнародна платіжна система до використання цих засобів. В Документах МПС також мають бути вказані найменування засобів захисту мережі, які використовуються, та надано копії чинних експертних висновків на них.

Якщо захищене з'єднання забезпечується шляхом створення VPN-каналу або HTTPS-з'єднання, це також має бути вказано. Для VPN-каналу необхідно зазначити технологію його створення (наприклад, IPSec), протокол (наприклад, ESP), алгоритми шифрування, механізм автентифікації та його алгоритм. Якщо використовується HTTPS-з'єднання, навести параметри шифрування. Наприклад: алгоритм ґешування SHA2, ключ шифрування RSA з довжиною 2048 біт, видавець сертифікату компанія N.

5. Опис криптографічних алгоритмів, протоколів та ключів

В Документах МПС в описі механізму шифрування інформації для обміну між учасниками та компонентами міжнародної платіжної системи рекомендовано зазначити алгоритми шифрування, довжину ключів та паролів. Якщо дані, що передаються, підписуються за допомогою електронного підпису (кваліфікований електронний підпис, удосконалений електронний підпис, MAC тощо), це також рекомендуємо вказати.

Особисті ключі, паролі та іншу конфіденційну інформацію необхідно передавати в захищеному від перегляду та модифікації вигляді. В Документах МПС слід зазначити порядок захисту такої інформації.

6. Опис процедури автентифікації

Оскільки обмін інформацією при використанні відкритих мереж повинен розпочинатися із взаємної автентифікації, в Документах МПС рекомендовано описати цей процес. Рекомендовано вказати, яка автентифікація (однофакторна чи двохфакторна) застосовується. Якщо для цього використовуються криптографічні методи, вказати за допомогою яких криптографічних засобів здійснюється автентифікація, за допомогою яких алгоритмів та з якою довжиною ключів.

Якщо використовується автентифікація за допомогою логіну та паролю, рекомендовано зазначити яким чином захищається передача паролю. У випадках, коли замість паролю передається його ґеш-функція, рекомендовано вказати алгоритм ґешування та довжину ґеш-функції. Якщо пароль до логіну є динамічним (наприклад, при використанні двохфакторної автентифікації), також це зазначити.

7. Рекомендації в частині використання електронного підпису

Відповідно до статті 18 Закону України “Про платіжні системи та переказ коштів в Україні” електронний підпис є обов’язковим реквізитом електронного документа на переказ, а учасник – резидент міжнародної платіжної системи має передбачити під час приймання електронних документів на переказ процедуру перевірки електронного підпису та процедуру перевірки цілісності, достовірності та авторства електронного документа на переказ. Виконання цієї вимоги можливо за допомогою створення/перевірки електронного підпису.

В Документах МПС рекомендовано зазначити вид електронного підпису, який використовується суб’єктом платіжного ринку для підпису електронного документа на переказ та під час створення архівів електронних документів на переказ. Рекомендовано описати на якому етапі, яким способом та за допомогою яких засобів створюється електронний підпис, де здійснюється перевірка цього підпису, яким чином виконується перевірка цілісності, достовірності та авторства електронного документу на переказ. Також вказати які криптографічні алгоритми та з якою довжиною ключів будуть використовуватись.

Під час підготовки Документів МПС рекомендовано врахувати, що порядок визнання іноземних електронних довірчих послуг та порядок використання іноземних сертифікатів відкритих ключів під час обміну електронними документами між суб’єктами міжнародної платіжної системи та учасниками – резидентами визначається вимогами законодавства України в сфері електронних довірчих послуг (розділ VI Закону України “Про електронні довірчі послуги”). Також іноземні сертифікати відкритих ключів можуть бути визнані шляхом укладанням договору між сторонами про взаємне визнання цих сертифікатів.

8. Створення архівів електронних документів

Під час формування, використання та зберігання архівів електронних документів на переказ, які створюються в МПС (далі – електронні архіви), повинна забезпечуватись їх цілісність, достовірність та авторство. Для цього під час формування електронних архівів для них створюється електронний підпис.

Рекомендовано зазначити, які засоби електронного підпису (вони повинні бути сертифіковані), криптографічні алгоритми та з якою довжиною ключів використовуються для перевірки цілісності, достовірності та авторства

даних під час формування, використання та зберігання електронних архівів учасниками – резидентами.

9. Взаємодія з іншими платіжними системами

Якщо договорами міжнародної платіжної системи передбачено здійснення переказу коштів за участю інших платіжних систем, в Документах МПС рекомендуємо вказати загальні вимоги щодо захисту інформації під час обміну інформаційними повідомленнями між платіжними системами, включаючи вимоги до технології обміну, порядку доступу, формування/перевірки електронних підписів, шифрування. Допускається в описі надавати загальні вимоги, наприклад, "для генерації та зберігання криптографічних ключів використовується технічний пристрій, що має чинний експертний висновок Держспецзв'язку".

Перелік законодавчих актів України, які необхідно використовувати під час розроблення документів міжнародної платіжної системи, платіжною організацією якої є нерезидент

I. Закони України:

- "Про платіжні системи та переказ коштів в Україні";
- "Про захист інформації в інформаційно-телекомунікаційних системах";
- "Про електронні довірчі послуги";
- "Про електронні документи та електронний документообіг";

II. Нормативно-правові акти:

- Положення про порядок реєстрації платіжних систем, учасників платіжних систем та операторів послуг платіжної інфраструктури, затверджене постановою Правління Національного банку України від 04.02.2014 № 43 (зі змінами);
- Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації, затверджене Наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20.07.2007 № 141 (зі змінами).