ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ

СПЕЦІНФОСИСТЕМИ

ЗАТВЕРДЖЕНИЙ
UA.32436187.00001-01 91 02-ЛЗ

КЛЮЧ ЕЛЕКТРОННИЙ DIAMOND

ІНСТРУКЦІЯ ЩОДО ПОРЯДКУ ГЕНЕРАЦІЇ КЛЮЧОВИХ ДАНИХ І ПОВОДЖЕННЯ З КЛЮЧОВИМИ ДОКУМЕНТАМИ

UA.32436187.00001-01 91 02

на 7 аркушах

Харків – 2022

ЗМІСТ

ЗАГАЛЬНІ ПОЛОЖЕННЯ

Інструкція щодо порядку генерації ключових даних і поводження з ключовими документами UA.32436187.00001-01 91 02 (далі – Інструкція) розроблена відповідно до вимог «Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту», затвердженого наказом Адміністрації Держспецзв'язку від 20.07.2007 № 141, зареєстрованим в Міністерстві юстиції України 20.07.2007 за № 862/14129 (зі змінами).

Ця Інструкція визначає вимоги та порядок генерації ключових даних і поводження (обліку, зберігання, знищення) з ключовими документами засобу криптографічного захисту інформації Ключ електронний DIAMOND (далі – Виріб).

Виріб призначений для захисту відкритої та конфіденційної інформації від загроз порушення її цілісності, конфіденційності, автентичності та неспростовності, яка надходить, зберігається та оброблюється в системах оброблення інформації.

Виріб може бути використаний для криптографічного захисту інформації з обмеженим доступом (крім інформації, що становить державну таємницю) та відкритої інформації, вимога щодо захисту якої встановлена законом.

Виріб може бути використаний в якості засобу кваліфікованого електронного підпису чи печатки для надання електронних довірчих послуг.

В Інструкції описані:

- ключові дані, що використовуються у Виробі;
- терміни дії та параметри ключових даних;
- порядок генерації та зберігання ключових даних;
- порядок використання ключових даних;
- порядок знищення ключових даних.

Норми даної Інструкції є обов'язковими для усіх користувачів Виробу.

Особи, винні в порушенні вимог цієї Інструкції, залежно від наслідків, притягуються до відповідальності відповідно до чинного законодавства.

1. КЛЮЧОВІ ДАНІ, ЩО ВИКОРИСТОВУЮТЬСЯ У ВИРОБІ

У Виробі використовуються наступні ключові дані:

- ДКЕ для ГОСТ 34.311-95;
- особисті та відкриті ключі алгоритму ДСТУ 4145-2002;
- особисті та відкриті ключі алгоритму RSA;
- особисті та відкриті ключі алгоритму ECDSA;
- особисті та відкриті ключі протоколу розподілу ключів Діффі-Геллмана на еліптичній кривій;
- таємні та сеансові (разові) ключі, нелінійні таблиці заміни для алгоритму блокового симетричного шифрування ДСТУ 7624:2014.
- таємні та сеансові (разові) ключі для алгоритму блокового симетричного шифрування AES;
- таємні та сеансові (разові) ключі для алгоритму блокового симетричного шифрування ДСТУ ГОСТ 28147:2009;
- довгостроковий ключовий елемент (далі – ДКЕ) алгоритму блокового симетричного шифрування ДСТУ ГОСТ 28147:2009 та алгоритму ґешування ГОСТ 34.310-95.

2. ТЕРМІНИ ДІЇ ТА ПАРАМЕТРИ КЛЮЧОВИХ ДАНИХ

2.1. Терміни дії ключових даних

Максимальний термін дії ключових даних (особистих та відкритих ключів) – 10 років.

Початок та завершення терміну дії ключових даних зазначаються у відповідному сертифікаті відкритого ключа. Строк чинності самого сертифіката (відкритих ключів) також зазначається у окремому полі сертифіката. Строк чинності сертифіката не може перевищувати термін дії особистого ключа.

2.2. Параметри ключових даних

3.2.1. Параметром ключових даних алгоритмів ДСТУ 4145-2002, ECDSA та протоколу розподілу ключів Діффі-Геллмана на еліптичній кривій є еліптична крива. Виріб має заздалегідь визначений перелік підтримуваних еліптичних кривих, який не може бути змінений користувачем. Підримуються наступні параметри:

- для алгоритму ДСТУ 4145-2002: еліптичні криві в поліноміальному базисі над розширеним полем визначені у ДСТУ 4145-2002 Додаток Г з m=257, m=307, m=367 та m=431;
- для алгоритму ECDSA: еліптичні криві над простим полем P-256, P-384, P-521, над розширеним полем K-233, B-233, K-283, B-283, K-409, B-409, K-571, B-571 визначені у NIST FIPS 186-4 Додаток D.
- протоколу розподілу ключів Діффі-Геллмана на еліптичній кривій: всі що наведені у переліку для алгоритмів ДСТУ 4145-2002 та ECDSA.

Користувач має вибрати еліптичну криву при генерації ключової пари для алгоритмів ДСТУ 4145-2002, ECDSA, протоколу розподілу ключів Діффі-Геллмана на еліптичній кривій виходячи з необхідного рівня стійкості.

3.2.2. Параметром ключових даних алгоритму RSA є довжина ключа. Виріб підтримує наступні довжини ключа RSA: 2048, 3072 та 4096 біт. Користувач має вибрати довжину ключа RSA при генерації ключової пари виходячи з необхідного рівня стійкості.

3.2.3. Параметрами ключових даних для алгоритму блокового симетричного шифрування ДСТУ 7624:2014 є довжина блоку шифру, довжина ключа та нелінійні таблиці заміни. Підтримуються наступні комбінації довжини блоку шифру та довжини ключа (в бітах): 128-128, 128-256, 256-256, 256-512, 512-512.

Нелінійні таблиці заміни для алгоритму ДСТУ 7624:2014 використовуються з Додатку А ДСТУ 7624:2014. Використання інших нелінійних таблиць заміни для алгоритму ДСТУ 7624:2014 можливе виключно за окремим погодженням Держспецзв’язку.

3.2.4. Параметром ключових даних для алгоритму блокового симетричного шифрування ДСТУ ГОСТ 28147:2009 є довгостроковий ключовий елемент (ДКЕ). У Виробі використовується ДКЕ № 1з Додатку 1 до «Інструкції про порядок постачання і використання ключів до засобів криптографічного захисту інформації», затвердженої наказом Адміністрації Держспецзв’язку від 12.06.2007 № 114, зареєстрованим в Міністерстві юстиції України 25.06.2007 за № 729/13996 (далі – Інструкція-114). Для алгоритму ґешування за ГОСТ 34.311-95 використовується ДКЕ № 1 з Інструкції-114. Використання інших ДКЕ можливе за окремим погодженням Держспецзв’язку або виключно для розшифрування/перевірки підпису вже інсуючих даних у разі якщо такий вказано в параметрах підписаного або зашифрованого документу або у складі сертифікату.

3.2.4. Параметром ключових даних для алгоритму блокового симетричного шифрування AES є довжина ключа. Підтримуються наступні довжини ключа: 128, 192 та 256 біт.

3. ПОРЯДОК ГЕНЕРАЦІЇ, ЗБЕРІГАННЯ ТА ЗНИЩЕННЯ КЛЮЧОВИХ ДАНИХ

Особисті ключі та відкриті ключі, таємні ключів блокових симметричних шифрів генеруються та знищуються користувачами за допомою вбудованих у Виріб засобів з використанням програмного забезпечення з комплекту поставки Виробу згідно Настанови щодо експлуатування.

Згенеровані особисті та таємні ключі автоматично записуються у захищену вбудовану пам'ять Виробу.

Згенеровані відкриті ключі включаються до складу запиту на формування сертифікату відкритих (Certificate Signing Request, CSR).

Сеансові (разові) ключі, призначені для шифрування даних, для алгоритмів ДСТУ 7624:2014, ДСТУ ГОСТ 28147:2009 та AES генеруються автоматично штатними засобами Виробу при зашифруванні відповідних даних та зберігаються разом із зашифрованими даними у зашифрованому на ключі, отриманому під час виконання протоколу розподілу ключів, вигляді.

При генерації особистих та таємних ключів користувачі повинні їх генерувати без можливості експорту з Виробу за виключенням технологічної необхідності, наприклад, необхідності створення резервних копій. Виключний перелік ключів, які дозволено генерувати з можливістю експорту, має бути встановлений наказом керівника організації, що експлуатує Виріб. Використовувати для роботи ключі з можливістю експорта заборонено.

Якщо є необхідність створення резервних копій особистих та таємних ключів рекомендується їх створювати наступним чином (всі роботи виконувати на відокремленій від мереж обміну даними ЕОМ з чистою операційною системою):

1) згенерувати необхідний ключ з можливістю експорта на Виробі;
2) за допомогою програмного забезпечення з комплекту поставки Виробу зробити необхідну кількість копій ключа, кожна з яких не має можливості експорту;
3) якщо створювати більше копій не буде потрібно – знищити ключ з можливістю експорту, інакше – забезпечити безпечне зберігання Виробу з ключем з можливістю експорту (наприклад, у сейфі відповідальної особи).

При генерації особистих та таємних ключів користувачі не повинні надавати дозвіл на їх використання без автентифікації за виключенням технологічної необхідності. Виключний перелік ключів, які дозволено генерувати з можливістю їх використання без автентифікації, має бути встановлений наказом керівника організації, що експлуатує Виріб.

Особисті та таємні ключі, у яких більше немає потреби, термін дії яких минув, або перед припиненням використання Виробу перед його поверненням, мають бути знищені користувачем за допомою вбудованих у Виріб засобів з використанням програмного забезпечення з комплекту поставки Виробу згідно Настанови щодо експлуатування.

При виведенні Виробу з експлуатації адміністратор безпеки має впевнитись що всі ключі та дані на Виробі знищені шляхом його форматування та встановлення випадкового пороля користувача.

4. ПОРЯДОК ВИКОРИСТАННЯ КЛЮЧОВИХ ДАНИХ

Для використання особистого або таємного ключа, що зберігається у вбудованій захищеній пам’яті Виробу, користувач авторизується на ньому шляхом введення свого паролю. Після правильного введення паролю Виріб та збережені у його пам’яті ключі можуть використовуватися за призначенням.

Введення паролю доступу повинно здійснюватися у спосіб, що не допускає ознайомлення з ним сторонніх осіб.

Після закінчення роботи користувач повинен завершити авторизовану сесію для унеможливлення несанкціонованого використання ключів, що зберігається у вбудованій захищеній пам’яті Виробу.