КРИПТОСОФТ
системы криптографической защиты

Засіб програмний КЗІ «Крипто підпис».

Обмежений сценарій використання – серверна частина

КРИПТОСОФТ
системы криптографической защиты

Опис сценарію

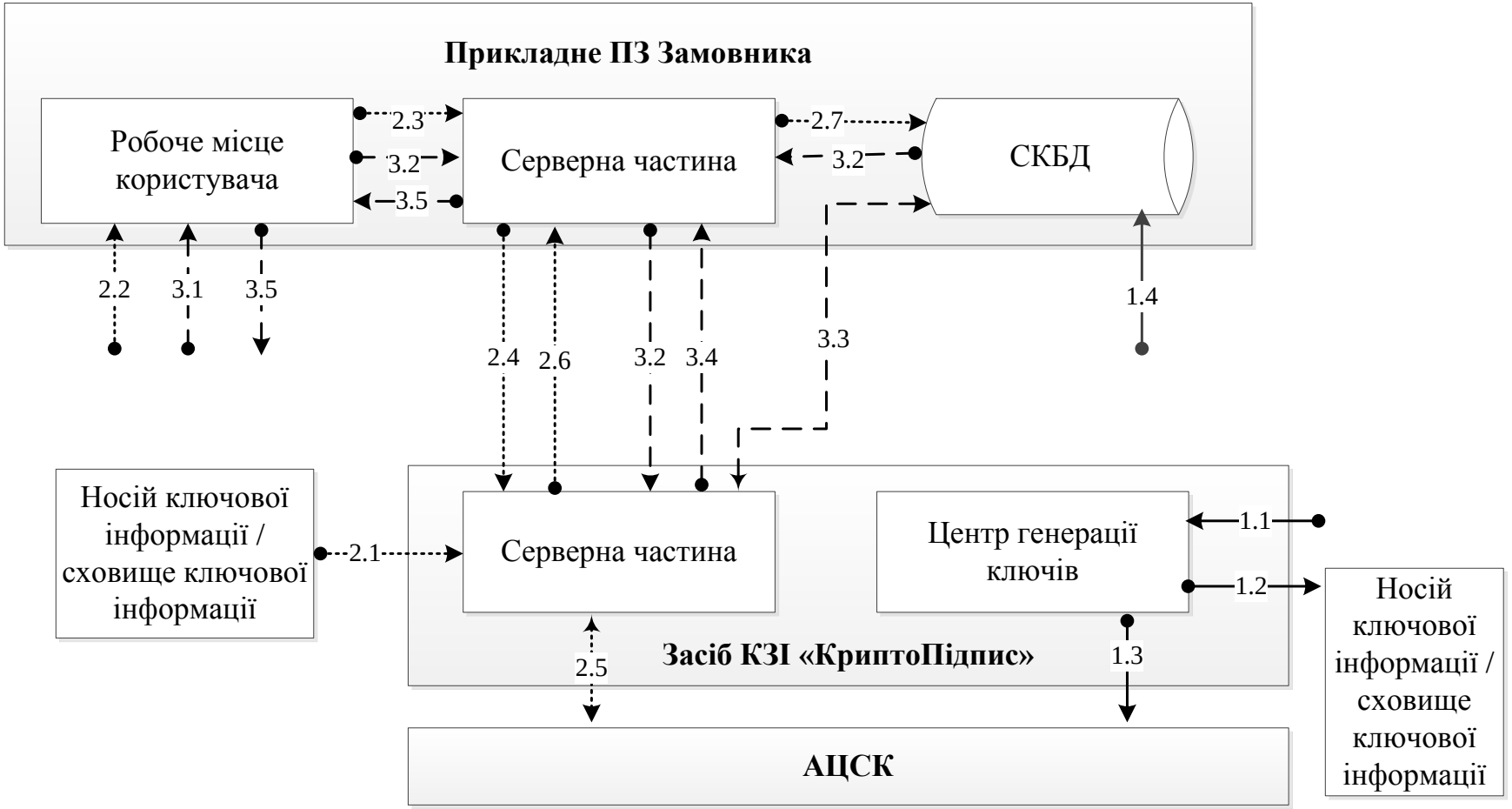
Загальні відомості

- Завдання: забезпечити можливість
  - автоматичного накладання електронного цифрового підпису (далі – ЕЦП) на документ з боку серверної частини прикладного програмного забезпечення Замовника;
  - перевірки ЕПЦ без інсталяції додаткового ПЗ на робочому місці Клієнта (можливість перевірки з будь-якого місця).
- Складові частини:
  - прикладне програмне забезпечення Замовника (веб-портал);
  - Програмний засіб КЗІ «КриптоПідпис» (далі – Засіб), виробництва ТОВ «СКЗ «Криптософт»

КРИПТОСОФТ
системы криптографической защиты

Архітектура та принцип роботи

Алгоритм функціонування



Алгоритм функціонування. Процес генерації ключових даних

1.1 Адміністратор (або інша відповідальна особа) ініціює процес формування криптографічних ключів ЕПЦ (особистий та відповідний йому відкритий ключ, запит до акредитованого центру сертифікації ключів (далі – АЦСК) на сертифікацію відкритого ключа) та вводить необхідні данні (пароль доступу до ключа, довжина ключа, тощо). Для виконання операції використовується Центр генерації ключів, що постачається разом с Засобом.

1.2 Сформований комплект ключів (закритий, відкритий ключі та запит до АЦСК на формування посиленого сертифіката відкритого ключа) зберігаються у визначене адміністратором місце.

Алгоритм функціонування. Процес генерації ключових даних

1.3 Виконується звернення до обраного АЦСК з метою формування та одержання посиленого сертифіката відкритого ключа. Порядок звернення визначається установленим в АЦСК порядком (Регламент роботи АЦСК). Для формування сертифіката Замовник надає до АЦСК запит на формування посиленого сертифікату відкритого ключа у форматі, що визначений стандартом PKCS# 10.

1.4 Сформований сертифікат завантажується у базу даних (або зберігається на жорсткий диск, або на токен) для подальшого використання у процесі функціонування системи.

Алгоритм функціонування. Процес накладання підпису

2.1 Адміністратор (відповідальна особа) завантажує носій ключової інформації та сертифікати (посилений сертифікат центрального засвідчувального органу, посилений сертифікат АЦСК, посилений сертифікат сервера позначок часу, посилений сертифікат з використанням ключа якого буде накладатися ЕЦП - уповноваженої особи) виконує запуск функціонування серверної частини Засобу (служби) та вводить пароль доступу до закритого ключа (з метою реалізації автоматизованого підпису).

2.2 Клієнт ініціює підписання документу (надає необхідні дані).

2.3 Система заповнює документ (додає до тексту типового договору персональні дані клієнта).

Алгоритм функціонування. Процес накладання підпису

2.4 Система надає визначений блок даних (документ) на підпис до серверної частини Засобу. Механізм надання даних на підпис реалізується розробником Системи із використанням консультаційної допомоги від ТОВ «СКЗ «Криптософт» та документації на Засіб.

2.5 Перед накладанням ЕЦП серверна частина Засобу звертається до АЦСК з метою встановлення факту, що посилений сертифікат відкритого ключа ЕЦП уповноваженої особи дійсний (чинний). У разі встановлення факту дійсності виконується обчислення значення ЕЦП на блок даних, що одержаний від Системи.

Здійснивши обчислення значення ЕЦП сервіс/сервер накладання та перевірки ЕЦП звертається до АЦСК з метою отримання позначки часу та отримавши її від АЦСК додає позначку часу (містить дату та час накладання ЕЦП), необхідну для встановлення факту підписання (створення) електронного документу.

Алгоритм функціонування. Процес накладання підпису

2.6 Виконується передача до Системи значення ЕЦП. Механізм одержання значення ЕЦП реалізується розробником Системи із використанням консультаційної допомоги від ТОВ «СКЗ «Криптософт» та документації на Засіб.

2.7 Система виконує збереження одержаного значення ЕЦП (наприклад, у базі даних).

До бази даних завантажується: безпосередньо документ (pdf файл) та підпис (p7s файл), що реалізується розробником Системи.

Алгоритм функціонування. Процес перевірки наявності підпису

3.1 Клієнт ініціює перевірку документу: визначає документ, перевірку якого необхідно виконати (форму вікна, спосіб відображення документів – завдання розробника Системи) та запускає процес перевірки натисканням кнопки (приклад: обирає файл pdf та p7s).

3.2 Система реагує на завдання Клієнта та надає дані для перевірки ЕЦП до серверної частини Засобу. Механізм реакції на натискання реалізується розробником Системи із використанням консультаційної допомоги від ТОВ «СКЗ «Криптософт» та документації на Засіб.

3.3 Серверна частина Засобу, із використанням посиленого сертифіката відкритого ключа (уповноваженої особи) який зберігається в БД, виконує перевірку значення ЕЦП та даних, що передаються на перевірку.

Алгоритм функціонування. Процес перевірки наявності підпису

3.4 Серверна частина Засобу надає позитивну / негативну відповідь, щодо дійсності значенні ЕЦП до таких даних (даних, що передавалися на перевірку та значення ЕЦП даних).

3.5 Визначена розробником Системи реакція на результати перевірки (у тому числі графічного відображення результатів перевірки ЕЦП Клієнту).

КРИПТОСОФТ
системы криптографической защиты

Особливості функціонування

Технічні особливості роботи серверної частини Засобу

- Серверна частина:
  - здійснює накладання та перевірку ЕЦП;
  - здійснює перевірку чинності посиленого сертифіката відкритого ключа сформованого АЦСК (за списками відкликаних сертифікатів або за сервісом інтерактивного визначення сертифіката) на момент обчислення (накладання/перевірки) ЕЦП;
  - здійснює автоматичне накладання ЕЦП на дані, що необхідно підписати ЕЦП;
  - здійснює отримання від АЦСК позначок часу на данні, що підписуються та поєднання позначок часу зі значенням ЕЦП;
  - за результатом перевірки ЕЦП віддає інформацію щодо дати та часу підписання ЕЦП (позначка часу), та інформацію, щодо підписанта (ким підписано).

КРИПТОСОФТ
системы криптографической защиты

Вимоги до апаратного та програмного забезпечення

Вимоги до апаратного та програмного забезпечення

- Мінімальні вимоги до апаратного та програмного забезпечення, яке потребує серверна частина Засобу:
  - Операційна система: Microsoft Windows (32/64 біт)
  - Віртуальна машина: JRE version 1.7.0 (від)
  - Центральний процесор: 1,6 МГц (від)
  - Оперативна пам'ять : 2048 Мб (від).

КРИПТОСОФТ
системы криптографической защиты

Контакти розробника

ТОВ "Системи криптографічного захисту "Криптософт“

м. Київ, Мельникова 83 А

тел.: (094) 92-90-179 або (044) 38-43-179

e-mail: Info@cryptosoft-ua.com

e-mail: support@cryptosoft-ua.com

www.cryptosoft-ua.com

КРИПТОСОФТ
системы криптографической защиты

Дякуємо за Вашу увагу!