КРИПТОСОФТ
системы криптографической защиты

Засіб програмний КЗІ «Крипто підпис»

Криптографічні алгоритми

- Засобом реалізовані наступні криптографічні алгоритми:
  - алгоритм шифрування даних відповідно до ДСТУ ГОСТ 28147:2009 у режимі гамування із зворотнім зв’язком
  - алгоритм обчислення імітовставки відповідно до ДСТУ ГОСТ 28147:2009
  - алгоритм обчислення геш-функції відповідно до ГОСТ 34.311-95;
  - алгоритми генерації параметрів, обчислення та перевіряння електронного цифрового підпису (ЕЦП) відповідно до ДСТУ 4145-2002;
  - алгоритм генерації псевдовипадкових послідовностей (ПВП) відповідно до Додатку А ДСТУ 4145-2002.
  - RFC 2631 "Diffie-Hellman Key Agreement Method", June 1999
  - та інші…

Потенційні замовники

- Державний сектор.
- Фінансовий сектор.
- Комерційний сектор.

- Державний сектор:
  - Системи електронного документообігу
  - Міжвідомчі автоматизовані системи обміну інформацією…
  - Системи та підсистеми електронного урядування
  - Системи подання адміністративних даних до органів державної влади
  - Портальні рішення (державні послуги, електронне самоврядування, державні закупівлі, звернення громадян, публічна влада, електронні медичні послуги, тощо).

e-gov ГОСУДАРСТВЕННЫЕ УСЛУГИ И ИНФОРМАЦИЯ ОНЛАЙН

ЭЛЕКТРОННОЕ ПРАВИТЕЛЬСТВО ГОСУСЛУГИ

Потенційні замовники

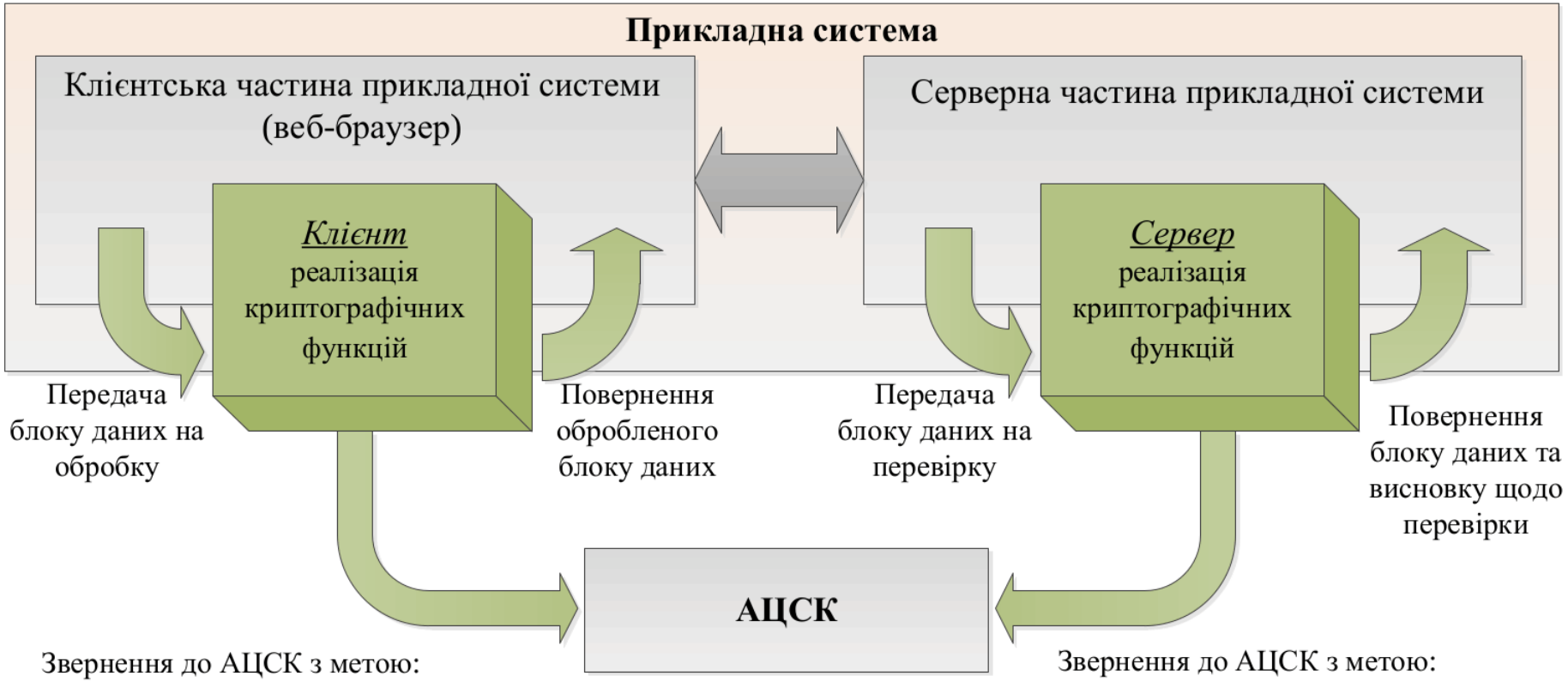
- Фінансовий сектор:
  - Електронні платіжні системи
  - Системи типу Клієнт-Банк (
  - Платіжні термінали (взаємодія з процесингом)
  - Системи електронного документообігу
  - АБС, ІБС, SAP, CRM – системи
- Комерційний сектор:
  - Електронні аукціони
  - Електронні торгові площадки
  - Фондові та валютні біржі
  - Медичні інформаційні системи
  - CRM – системи
  - Інформаційні системи страхових компаній
  - Торгівельні системи
  - Інформаційні системи недержавних пенсійних фондів

КРИПТОСОФТ
системы криптографической защиты

Архітектура та принцип роботи Засобу

- Архітектура Засобу
- Складові частини Засобу

Архітектура Засобу

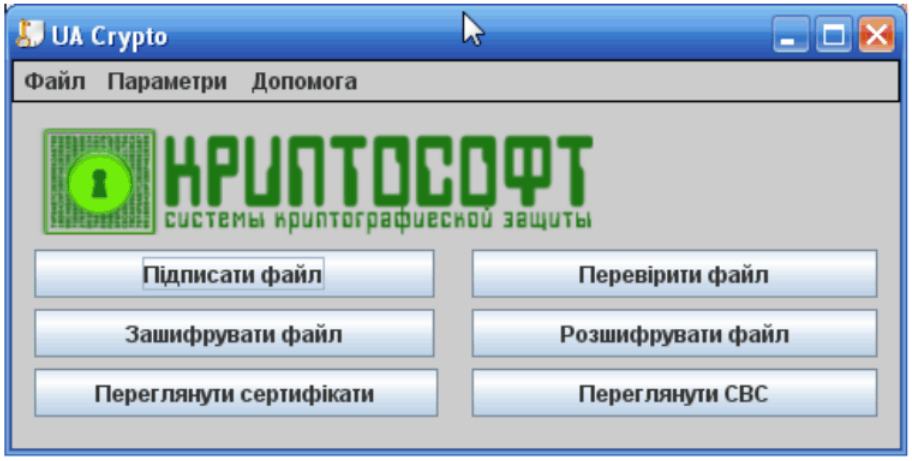


Складові частини Засобу

- Серверна частина;
- Клієнтська частина:
  - «Товстий клієнт»;
  - ВЕБ - апплет.
- Серверна частина забезпечує:
  - накладання та перевірку ЕЦП
  - шифрування та дешифрування інформації
  - перевірку статусу сертифіката за механізмом списку відкликаних сертифікатів (CRL)
  - перевірку статусу сертифіката у режимі реального за механізмом інтерактивного визначення статусу сертифіката
  - отримання позначки часу (TSP)
  - підключення файлового токену, смарт-карти або USB-токену
  - забезпечує інтерфейс взаємодії з сторонніми прикладними системами Замовника за протоколом SOAP

Складові частини Засобу

- Серверна частина.
- Клієнтська частина:
  - «Товстий клієнт»;



  - ВЕБ – апплет.

Серверна частина Засобу. Основні функції

- Серверна частина забезпечує:
  - накладання та перевірку ЕЦП
  - шифрування та дешифрування інформації
  - перевірку статусу сертифіката за механізмом списку відкликаних сертифікатів (CRL)
  - перевірку статусу сертифіката у режимі реального за механізмом інтерактивного визначення статусу сертифіката (OCSP)
  - отримання позначки часу (TSP)
  - підключення файлового токену, смарт-карти або USB-токену
  - забезпечує інтерфейс взаємодії з сторонніми прикладними системами за протоколом SOAP

Серверна частина Засобу. Особливості

- Функціонує у вигляді служби (сервісу);
- Забезпечує взаємодію з прикладним програмним забезпеченням Замовника;
- Здатна функціонувати самостійно, як незалежна складова прикладної системи Замовника, наддаючи можливість використання всього функціоналу за допомогою визначених та описаних інтерфейсів взаємодії з прикладним ПЗ Замовника.

Клієнтська частина Засобу. Основні функції

- Клієнтська частина Засобу забезпечує:
  - генерацію ключових даних (криптографічних ключів)
  - формування запиту на сертифікацію відкритого ключа до АЦСК
  - накладання та перевірку ЕЦП
  - шифрування та дешифрування інформації
  - перевірку статусу сертифіката за механізмом списку відкликаних сертифікатів (CRL)
  - перевірку статусу сертифіката у режимі реального за механізмом інтерактивного визначення статусу сертифіката (OCSP)
  - отримання позначки часу (TSP)
  - підключення файлового токену, смарт-карти або USB-токену

КРИПТОСОФТ
системы криптографической защиты

Опис Засобу

- Загальні відомості
- Призначення
- Необхідність використання Засобу
- Переваги Засобу
- Криптографічні алгоритми
- Потенційні Замовники та приклади прикладних завдань, для вирішення яких призначений Засіб

ВЕБ-апплет. Особливості

- Забезпечує взаємодію з прикладним програмним забезпеченням Замовника;
- Забезпечує можливість реалізації аутентифікації користувача в системі за наявності в нього відповідних ключових даних та сертифіката відкритого ключа;
- Забезпечує можливість реалізації національних криптографічних стандартів у ВЕБ – додатках з використанням провідних ВЕБ – оглядачів (Google Chrome, Mozilla Firefox, Opera, Internet Explorer);
- Здатний функціонувати самостійно, надаючи користувачу можливість використання всього функціоналу за допомогою графічного інтерфейсу користувача.

«Товстий клієнт». Особливості

- Функціонує окремо від прикладного ПЗ Замовника;
- Виконаний у вигляді файлу, що запускається (exe-файл);
- Забезпечує можливість реалізації аутентифікації користувача в системі за наявності в нього відповідних ключових даних та сертифіката відкритого ключа;
- Здатний функціонувати самостійно, надаючи користувачу можливість використання всього функціоналу за допомогою графічного інтерфейсу користувача.

КРИПТОСОФТ
системы криптографической защиты

Ліцензійна політика

- Демонстраційна
- Обмежена
- Повнофункціональна

Існуючи варіанти ліцензійної політики

- Демонстраційна:
  - призначена для надання можливості потенційному Замовнику ознайомитись з можливостями Засобу.
  - функціональні обмеження відсутні, у порівнянні з обмеженою політикою.
  - забороняється використовувати у складі автоматизованих систем, в яких побудовано комплексну систему захисту інформації.

- Обмежена:
  - Призначена для надання можливості використання Засобу в процесах забезпечення життєдіяльності Замовника з єдиним обмеженням: заблоковано функцію Клієнтської та серверної частин виконувати генерацію ключових даних.

Існуючи варіанти ліцензійної політики

- Повнофункціональна:
  - Призначена для надання можливості використання Виробу без обмеження в процесах забезпечення життєдіяльності Замовника.

КРИПТОСОФТ
системы криптографической защиты

Сценарії використання

Централізована схема генерації ключових даних

- Використовується обмежена ліцензійна політика на Засіб;
- Генерація ключових даних виконується центральними підрозділами Замовника за допомогою Засобу КЗІ «Центр генерації ключів, v.3», розробки ТОВ «СКЗ «Криптософт»;
- Розповсюдження закритого ключа користувача виконується відповідно до прийнятих у Замовника процедур;
- Звернення до АЦСК з метою формування сертифікату відкритого ключа виконується централізовано, відповідно до прийнятих у Замовника процедур.

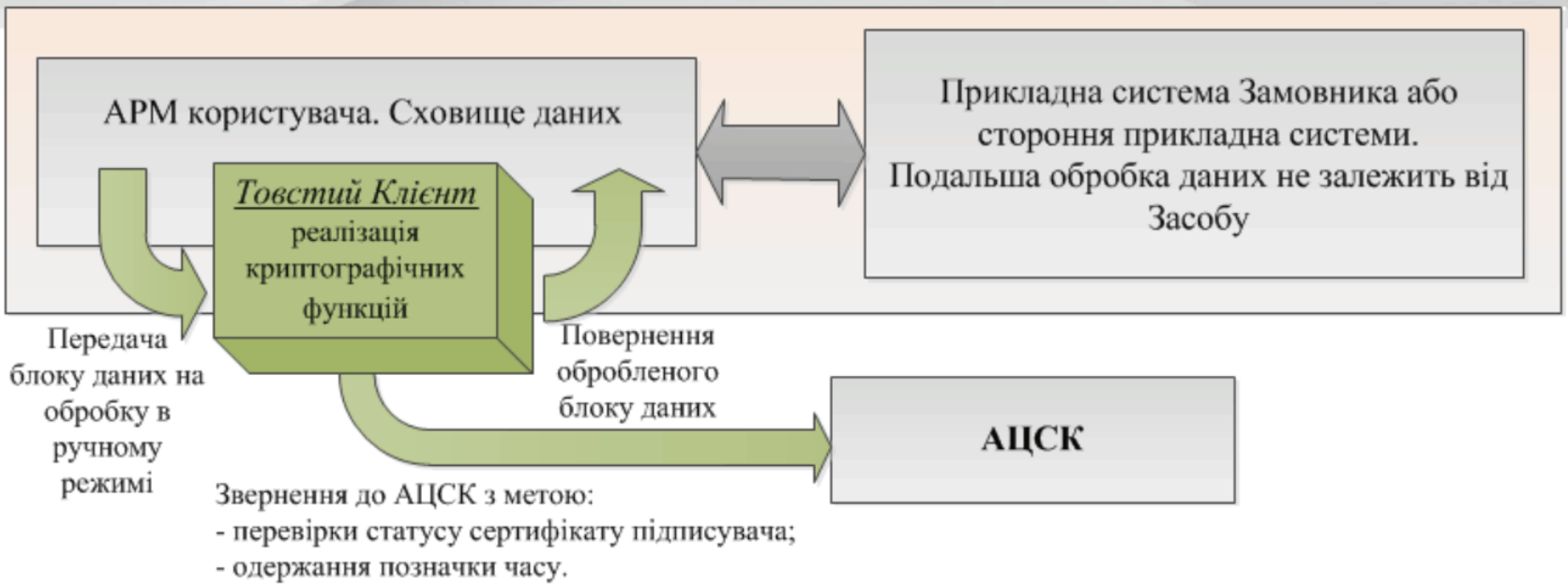
Децентралізована схема генерації ключових даних

- Використовується повнофункціональна ліцензійна політика на Засіб;
- Генерація ключових даних виконується користувачем клієнтської частини із використанням її (клієнтської частини) можливостей;
- Звернення до АЦСК з метою формування сертифікату відкритого ключа виконується децентралізовано, відповідно до прийнятих у Замовника процедур.

Сценарій повного використання Засобу

- Повністю відповідає архітектурі Засобу.
- Використовується у випадку, якщо:
  - користувачам-клієнтам прикладної системи Замовника необхідно виконати будь-які криптоперетворення з даними, що циркулюють в даній прикладній системі.
  - серверна частина прикладної системи Замовника повинна виконати перевірку справжності виконаних на клієнтському місці криптоперетворень перед тим, як виконати з одержаними даними будь-які визначені розробником дії.

Сценарій обмеженого використання Засобу. «Товстий клієнт»

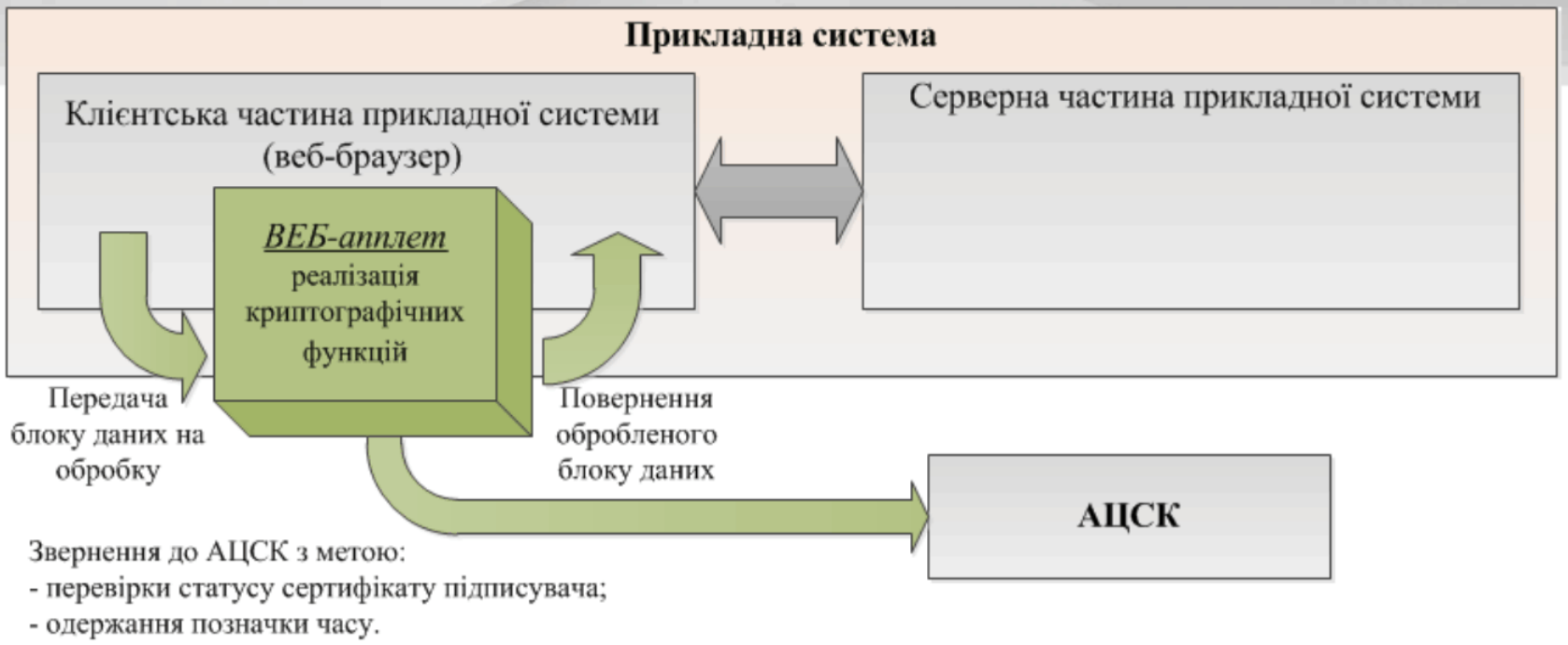


- В даному сценарії задіяний виключно «товстий клієнт».
- Використовується у випадку, якщо Замовнику необхідно виконати криптографічні перетворення (накладання / перевірка ЕЦП, шифрування / дешифрування) над даними, спосіб передачі яких до власної (або сторонньої) прикладної системи виконується у ручному режимі. Наприклад: документ , підписаний ЕЦП, передається до іншої організації засобами електронної пошти.

Загальні відомості

- Засіб є розробкою ТОВ «Системи криптографічного захисту «Криптософт»
- Засіб функціонує в середовищі віртуальної Java-машини (JVM) незалежно від комп'ютерної архітектури (кросплатформений)
- Засіб перебуває на етапі проходження державної експертизи в сфері криптографічного захисту інформації та найближчим часом отримає позитивний експертний висновок Держспецзв’язку

Сценарій обмеженого використання Засобу. ВЕБ-апплет



- В даному сценарії задіяний виключно ВЕБ-апплет.
- Використовується у випадку, якщо користувачам-клієнтам прикладної системи Замовника необхідно виконати будь-які криптоперетворення з даними, що циркулюють в даній прикладній системі, яка являє собою ВЕБ-портал. При цьому на серверну частина прикладної системи Замовника не покладається жодних функцій з перевірки справжності виконаних на клієнтському місці криптоперетворень перед тим, як виконати з одержаними даними будь-які визначені розробником дії.

Сценарій обмеженого використання Засобу. Серверна частина

- В даному сценарії задіяний виключно серверна частина Засобу.
- Використовується у випадку, якщо Замовнику неважливо, яким чином було виконано криптоперетворення над даними, що передаються до серверної частини прикладної системи Замовника.
- При цьому серверна частина прикладної системи Замовника повинна виконати перевірку справжності виконаних криптоперетворень перед тим, як виконати з одержаними даними будь-які визначені розробником дії.

КРИПТОСОФТ
системы криптографической защиты

Контакти розробника

ТОВ "Системи криптографічного захисту "Криптософт“

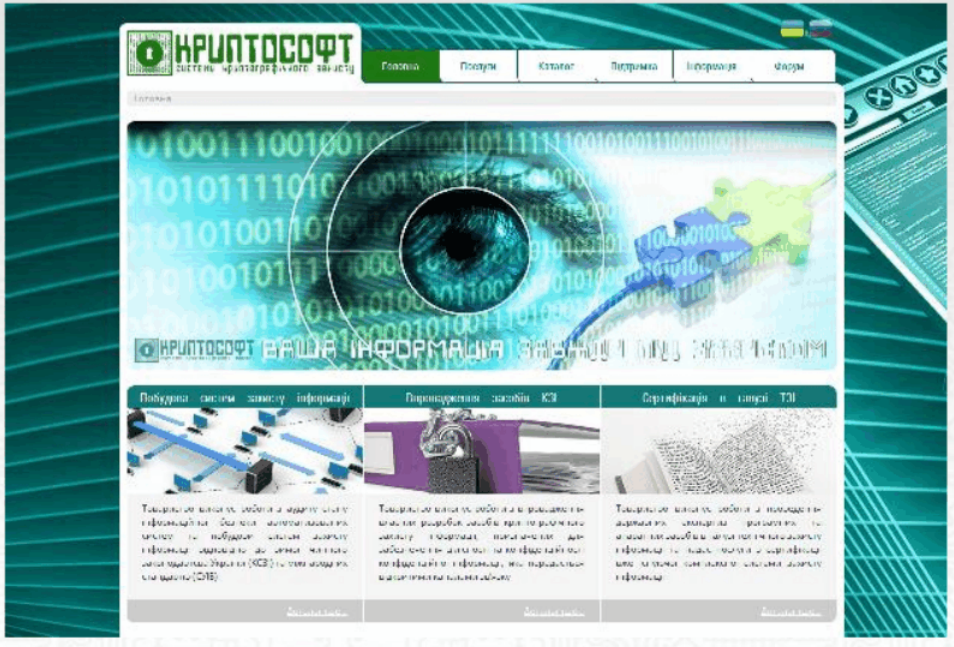
м. Київ, Мельникова 83 А

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!

Призначення

- Забезпечення цілісності інформації та підтвердження авторства шляхом використання механізмів електронного цифрового підпису (накладання та перевірка підпису)
- Забезпечення конфіденційності інформації, яка передається незахищеними каналами зв'язку (Інтернет), шляхом використання механізмів шифрування (шифрування та дешифрування інформації)
- Забезпечення взаємодії з акредитованими центрами сертифікації ключів з метою отримання послуг електронного цифрового підпису
- Забезпечення криптографічного захисту інформації, яка має максимальний гриф обмеження доступу – ***конфіденційно*** (персональні данні, комерційна та банківська таємниця, тощо)

Необхідність використання Засобу

- Вимоги чинного законодавства України та підзаконних нормативно-правових актів

- Необхідність забезпечення цілісності інформації, яка циркулює в інформаційній системі та підтвердження її авторства, шляхом обчислення значення електронного цифрового підпису

- Необхідність забезпечення конфіденційності інформації, яка циркулює в інформаційній системі або передається між її складовими частинами з використанням відкритих каналів зв'язку (Інтернет), шляхом здійснення криптографічного перетворення такої інформації

Переваги Засобу

ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

ЕКСПЕРТНИЙ ВИСНОВОК

- **масштабованість**: можливість використовувати компоненти Засобу з урахуванням архітектури приладного програмного забезпечення, у складі якого використовується Засіб;
- **простота забезпечення вимог з сертифікації засобів КЗІ:** Засіб є органічним та цілісним програмним продуктом, який відповідає чинній нормативній базі України в галузі КЗІ та може використовуватись у складі прикладного ПЗ Замовника, як його складова частина, без необхідності проведення державної експертизи в галузі КЗІ прикладного ПЗ Замовника на правильність вбудовування криптофункцій;
- **перевірені режими взаємодії з АЦСК:** можливість отримання послуг ЕЦП від провідних АЦСК України, а саме: Міністерства доходів і зборів України, Українського сертифікаційного центру, Державної казначейської служби України, Національного депозитарію України, Masterkey та інші.

Переваги Засобу

- **мобільність та простота установки**:
  - зручність та простота налаштування як клієнтської, так і серверної складової Засобу (налаштування зберігаються у конфігураційних файлах),
  - можливість функціонування складових частин Засобу у складі віртуальних машин (Oracle VM VirtualBox, VMware, Microsoft Hyper-V, Citrix Xen, інші)

- **кроссплатформеність**:
  - можливість функціонування складових частин Засобу під управлінням операційних систем як сімейства Windows так і операційних систем сімейства Linux/Unix, що забезпечується середовищем віртуальної Java-машини (JVM).
  - виконання криптографічних перетворень в середовищі віртуальної Java-машини забезпечує підтримку:

Microsoft Windows XP, Vista, 7,8, 2003, 2008, 2012 (та нові версії, які будуть підтримувати Java)

Linux Red Hat, CentOS, Ubuntu, SUSE, Debian (інші версії, які підтримують Java)

BSD-UNIX (FreeBSD, OpenBSD) (інші версії, які підтримують Java)

Переваги Засобу

- **Простота інтеграції** Засобу в існуючі інформаційні системи, а також в системи, які створюються шляхом надання розробникам інформаційних систем комплекту документації, що у обов'язковому порядку містить опис функцій та приклади їх застосування.

- Можливість виклику функцій, які забезпечують накладання та перевірку електронного цифрового підпису (ЕЦП) за наступними типами форматів: «Базовий ЕЦП».

- **Відповідність вимогам чинного законодавства України**, підзаконним нормативно-правовим актам, державним стандартам (ДСТУ ISO/IEC, ДСТУ ETSI TS), міжнародним стандартам криптографії з відкритим ключем (PKCS), робочим пропозиціям (RFC)…

Переваги Засобу

- Можливість зберігання ключових даних (криптографічних ключів) як у складі файлового контейнера, так і на носії ключової інформації типу смарт-карта або USB-токені (PKCS#11);

- Програмна генерація ключових даних при використанні файлового контейнера, забезпечує зручність створення резервних копій ключових даних шляхом резервування файлового контейнера в цілому;

- Апаратна генерація ключових даних при використанні смарт-карти або USB-токену забезпечує формування ключових даних на пристрої, а також унеможливлює експортування ключових даних з пристрою