БЪЛГАРСКА ФОНДОВА БОРСА - СОФИЯ

БЪЛГАРСКА ФОНДОВА БОРСА
СОФИЯ

ТЕХНИЧЕСКА ПРОЦЕДУРА ОТНОСНО МЕХАНИЗМИТЕ ЗА СИГУРНОСТ ПРИ КРИПТИРАНЕ НА ДАННИ, ЗАЩИТА ПРИ ГЕНЕРИРАНЕ И СЪХРАНЕНИЕ НА СЕРТИФИКАТИ И УСЛОВИЯТА ПРИ РАЗПРОСТРАНЕНИЕ НА ИНФОРМАЦИЯ ЗА ВАЛИДНОСТТА НА СЕРТИФИКАТИТЕ ОТ БФБ-СОФИЯ АД

Процедури при генериране на електронни сертификати от Борсата

1. Във връзка с осигуряването на необходимата степен на защита и сигурност при търговията чрез COBOS, абонатите на Борсата и доверяват създаването и определянето на електронни сертификати (ключове) на отделните потребители.
2. Издадените от Борсата ключове се използват за подписване на електронни сертификати (сертификати) и служат за идентифициране като конкретния потребител (обект). Електронният сертификат свързва публичния ключ към физическо лице или организация. Свързването се потвърждава от доверен източник.
3. При изграждането на системата COBOS, Борсата в качеството си на доставчик на услуги за сигурност при електронен обмен на данни, който издава сертификати с ограничено приложение, създава собствен Сертификационен агент, подписващ сертификатите на обектите и сертификата на COBOS-сървъра.
4. Достъп до системата COBOS получават само потребители, притежаващи валидни сертификати, подписани от COBOS в качеството му на Сертификационен агент. В зависимост от сертификата, на абонатите се предоставя различен достъп до наличната информация в COBOS, както и до видовете действия, които могат да извършват.
5. Сертификата съдържа информация за името на притежателя, e-mail адрес, географско разположение, валидност на сертификата. Освен това, в сертификата се съдържа и публичния ключ и уникална стойност (hash), която удостоверява, че сертификата не е бил променян.
6. Уникалната стойност представлява число, извлечено посредством прилагане на алгоритъм за уникалност (hash-algorithm). Прилагането на алгоритъма върху съобщението не позволява да се възстанови оригиналното съобщение от уникалната стойност.
7. При промяна на съобщението уникалната стойност се променя. По този начин се гарантира, че трето неоторизирано лице, не може да промени незабелязано съобщение, което да запази оригиналната си уникална стойност.
8. Издаването на сертификат на потребител, посредством COBOS или по друг определен от Борсата начин, преминава през следните стъпки:
    - 8.1. Обектът изпраща заявка към Борсата за издаване на сертификат. Посочената заявка генерира CRS файл (Certificate Signed Request), в който се съдържа следната минимална информация:
        - 8.1.1. Име на притежателя;
        - 8.1.2. ЕГН/БУЛСТАТ;
        - 8.1.3. Номер на документа за самоличност/Данъчен номер;
        - 8.1.4. Град;
        - 8.1.5. Код на държавата;
        - 8.1.6. Крайна дата на валидност на сертификата;
        - 8.1.7. E-mail адрес.
    - 8.2. Съответният администратор в COBOS регистрира потребителя и му задава права.
    - 8.3. Администратор на Сертификационния агент по т. 9 проверява за коректност

при регистрация и за идентичност с информация, подадена в хартиеното заявление до Борсата.

8.4. Администратор на Сертификационния агент стартира генериране на сертификат.

8.5. Сертификатът, подписан от Борсата и преобразуван във вид за инсталиране в браузера, се изпраща по електронна поща, на посочения при регистрацията e-mail адрес, до неговия притежател.

Процедури относно защита и съхранение на сертификати и условията за разпространение на информация за валидността на сертификатите от Борсата

9. Генерирането и съхраняването на ключове от Борсата се извършва във физически сигурна среда от упълномощени служители на Борсата (администратори на Сертификационния агент) под най-малко двоен контрол. Служителите се упълномощават със заповед на изпълнителния директор на Борсата.

10. Въведените от абоната данни се съхраняват на подсигурен сървър в Борсата, в случай че сертификата трябва да бъде подновен.

11. Частните ключове на всички абонати се генерират автоматично и съхраняват на подсигурен сървър в Борсата.

12. Частният ключ на COBOS се съхранява на подсигурен сървър в Борсата.

13. Достъп както до частния ключ на COBOS, така и до частните ключове на абонатите, се получава след въвеждане на пароли от двама независими един от друг администратори на Сертификационния агент.

14. Борсата поддържа списък на отменените сертификати (Certificate Revocation List), чиято валидност не е изтекла, но поради друга причина те не са валидни, който се съхранява на подсигурен сървър. След края на всяка търговска сесия Борсата публикува списъка на отменените сертификати.

15. Подсигуреният сървър се организира по следният начин:

15.1. Забранява се достъпът до него по всякаква мрежа като се допуска единствено HTTPS връзка за работа в COBOS;

15.2. Частните ключове и сертификатите се съхраняват в криптиран вид, подписани с частния ключ на Борсата, в дублирана файлова организация (в две различни дървовидни структури на директории);

15.3. Информацията за частните ключове и сертификатите се записва едновременно на две огледални двойки твърди дискове, инсталирани на сървъра.

Процедури при изграждане на криптирана връзка между обекта и сървъра на Борсата

16. При криптирането се използва двойка публичен/частен ключ, която гарантира че данните криптирани с един публичен ключ могат да бъдат прочетени само от един, точно определен, частен ключ (двойка асиметрични ключове).

17. Използването на един и същ ключ за криптиране и декриптиране не е възможно.
18. Изграждането и обмена на информация между обекта и сървъра преминава през следните стъпки:

18.1. Браузърът на обекта отправя запитване на подсигурения сървър (Secure HTTP server)

18.2. Обектът изпраща своя публичен ключ към сървъра.

18.3. Сървърът проверява идентичността на обекта посредством проверка на сертификата. Проверката обхваща валидността му и дали е подписан от трета доверена страна. Ако сертификатът е изтекъл или е подписан от недоверена страна, сървърът изпраща предупредително съобщение и прекратява връзката.

18.4. Сървърът изпраща своя публичен ключ и своя сертификат.

18.5. Браузърът проверява, че сертификатът е валиден и подписан от доверена страна (root Certificate Authority)

18.6. Барузърът използва публичния ключ за криприране на случаен симетричен ключ и го изпраща към сървъра, заедно с желаните данни.

18.7. Сървърът декриптира симетричния ключ за декриптиране на данните.

18.8. Сървърът изпраща обратно данните, изискани от браузъра, като ги криптира със симетричния ключ.

18.9. Браузърът декриптира данните, използвайки симетричния ключ и визуализира информацията.