ПРАВИЛА
ЗА ИЗДАВАНЕ И СЪХРАНЕНИЕ НА КЛИЕНТСКИ СЕРТИФИКАТИ ЗА РАБОТА СЪС СИСТЕМАТА КАРОЛ БРОКЕР

Процедури при генериране на електронни сертификати от Карол

1.Във връзка с осигуряванетона необходимата степен на защита и сигурност при търговията чрез КАРОЛ БРОКЕР, абонатите на Карол и доверяват създаването и определянето на електронни сертификати (ключове) на отделните потребители.

2. Издадените от Карол 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 КАРОЛ БРОКЕР, Карол в качеството си на доставчик на услуги за сигурност при електронен обмен на данни, който издава сертификати с ограничено риложение, създава собствен Сертификационен агент /Karoll CA/ ,подписващ сертификатите на обектите и сертификата на КАРОЛ БРОКЕР-сървъра.

4. Достъп до системата КАРОЛ БРОКЕР получават само потребители, притежаващи валидни сертификати, издадени от Карол в качеството му на Сертификационен агент. В зависимост от сертификата, на абонатите се предоставя различен достъп до наличната информация в КАРОЛ БРОКЕР, както и до видовете действия, които могат да извършват.

5. Сертификата съдържа информация за името на притежателя, e-mail адрес, уникален клиентски номер, валидност на сертификата и тип 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 КАРОЛ БРОКЕР или по друг определен от Карол начин, преминава през следните стъпки:

8.1. Обектът изпраща заявка към Карол за издаване на сертификат. Посочената заявка съдържа следната минимална информация:

- 8.1.1. Email адрес
- 8.1.2. Име на притежателя
- 8.1.3.Клиентски номер
- 8.1.4. Тип на сертификата
- 8.1.5. Валидност на сертификата

8.2. Съответният администратор в КАРОЛ БРОКЕР регистрира потребителя и му задава права.

8.3. Администратор на Сертификационния агент по т. 9 проверява за коректност при

регистрация и за идентичност с информацията в клиентския регистър

8.4. Администратор на Сертификационния агент стартира генериране на сертификат

8.5.Сертификатът, подписан от Карол 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 Карол

9. Генерирането и съхраняването на ключове от Карол се извършва във физически сигурна среда от упълномощени служители на Карол (администратори на Сертификационния агент). Служителите се упълномощават със заповед на изпълнителния директор на Карол.

10. Въведените от абоната данни се съхраняват в клиентския регистър в Карол, в случай че сертификата трябва да бъде подновен.

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

12. Частният ключ на КАРОЛ БРОКЕР се съхранява на подсигурен сървър в Карол.

13. Достъп както до частния ключ на КАРОЛ БРОКЕР, така и до частните ключове на абонатите се получава след въвеждане на пароли както за самия сертификат така и за достъп до сървъра със съхраняваните сертификати от администраторите на Сертификационния агент.

14. Карол 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.

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

15. 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).

16. Използването на един и същ ключ за криптиране и декриптиране не е възможно.

17. Изграждането и обмена на информация между обекта и сървъра преминава през следните стъпки:

17.1. Приложението на клиента отправя запитване на подсигурения сървър

17.2. Обектът изпраща своя публичен ключ към сървъра.

17.3. Сървърът проверява идентичността на обекта посредством проверка на сертификата. Проверката обхваща валидността му и дали е подписан от трета доверена страна, дали съвпадат посочените потребител и парола със тези, записани в базата данни. Ако сертификатът е изтекъл или е подписан от недоверена страна, или има някакво друго несъответствие, сървърът изпраща предупредително съобщение и прекратява връзката.