УСЛОВИЯ, РЕД И НАЧИН

ЗА ИЗПОЛЗВАНЕ НА
КВАЛИФИЦИРАН ЕЛЕКТРОНЕН ПОДПИС
И
УДОСТОВЕРЕНИЕ ЗА ВРЕМЕ

Версия 2.0

Март, 2016 г.

СЪДЪРЖАНИЕ

ИЗПОЛЗВАНИ СЪКРАЩЕНИЯ И ТЕРМИНИ 3
ВЪВЕДЕНИЕ 4
I. УСЛОВИЯ, РЕД И НАЧИН НА ИЗПОЛЗВАНЕ НА КВАЛИФИЦИРАН ПОДПИС 5
1. Общи правила на използване на подписа 5
2. Правила при подписване 5
3. Начин на използване - проверени софтуерни приложения 6
4. Ограничения при употреба на подписа 6
5. Задължения на Автора и на Титуляря при подписване 7
6. Техническа сигурност и контрол 7
7. Тайна на частния ключ 7
8. Генериране на нова двойка ключове 7
9. Компрометиране на частния ключ 8
10. Унищожаване на частен ключ 8
11. Активиране и деактивиране на частен ключ 8
II. ПРИЕМАНЕ НА ПОДПИСА 8
1. Доверие в електронния подпис 8
2. Дължима грижа на Доверяваща се страна 9
III. УСЛОВИЯ, РЕД И НАЧИН НА ИЗПОЛЗВАНЕ НА УДОСТОВЕРЕНИЕ ЗА ВРЕМЕ 11
1. Общи правила 11
2. Издаване на УВ 11
3. Начин на използване на УВ 11
4. Ограничаване при употреба на УВ 12
5. Задължение на страните при употреба на УВ 12
6. Техническа сигурност и контрол 12
IV. ПРИЕМАНЕ НА УДОСТОВЕРЕНИЕ ЗА ВРЕМЕ 13
1. Доверие в УВ 13
2. Дължима грижа на Доверяваща се страна 13

Използвани съкращения и термини

На английски език:

B-Trust®	Търговска марка на дейността на „Борика-Банксервиз” АД като ДУУ
CA	Certificate Authority – Удостоверяващ орган
CRL	Certificates Revocation List – Списък на прекратени удостоверения
ETSI	European Telecommunications Standard Institute – Европейски институт за телекомуникационни стандарти
FIPS	Federal Information Processing Standard – Федерален Стандарт за обработка на информация
ISO	International Standard Organization – Международна Организация по стандарти
OID	Object Identifier – Идентификатор на обект
OCSP	On-line Certificate Status Protocol – Протокол за проверка на статус на удостоверение в реално време
PKCS	Public Key Cryptography Standards – Криптографски Стандарти на публични ключове
PKI	Public Key Infrastructure – Инфраструктура на публични ключове
RA	Registry Authority – Регистриращ орган
RSA	Rivers-Shamir-Adelman – Криптографски алгоритъм (асиметричен)
SSCD	Secure Signature Creation Device –Устройство за създаване на сигурен електронен подпис
SHA	Secure Hash Algorithm – Хеш функция
SSL	Secure Socket Layer – Защитена HTTP сесия
TSA	Time Stamp Authority – Орган на удостоверения за време
TST	Time Stamp Token – Удостоверение за време

На български език:

АД	Акционерно дружество
ДУУ	Доставчик на Удостоверителни Услуги
ЗЕДЕП	Закон за електронния документ и електронния подпис
ЗЕУ	Закон за Електронно Управление (е-Управление)
КРС	Комисия за регулиране на съобщенията
МРС	Местна Регистрираща Служба
НДДУУ	Наредба за дейността на доставчиците на удостоверителни услуги
НИАКЕП	Наредба за изискванията към алгоритмите за квалифицира електронен подпис
Наръчник	Наръчник на потребителя за предоставяните от "БОРИКА - БАНКСЕРВИЗ" АД B-TRUST® удостоверителни, информационни, криптографски и консултантски услуги за квалифициран електронен подпис
Практика	Практика на предоставяне на удостоверения за квалифициран електронен подпис, Практика на органа за удостоверяване на време
Политика	Политика на предоставяне на удостоверения за квалифициран електронен подпис, Политика на органа за удостоверяване на време
КЕП	Квалифициран Електронен Подпис

Въведение

Настоящият документ описва:

- Начинът на използване на квалифицирания електронен подпис (КЕП), за който е издадено съответно квалифицирано удостоверение на Автор/Титуляр, както и начинът на използване на издаваните удостоверения за време от ДУУ „БОРИКА-БАНКСЕРВИЗ” АД;
- Условията и реда за използване на КЕП, включително изискванията за съхраняване на частния ключ на Автора/Титуляря, както и условията и реда за използване на удостоверенията за време;
- Условията за достъп до удостоверение за КЕП и удостоверение за време, както и начинът на проверка на КЕП и удостоверението за време.

На базата на този документ, всеки Автор/Титуляр на удостоверения за КЕП и/или Доверяваща се страна на КЕП и на удостоверение за време може да дефинира, създаде и следва конкретна Политика на подписване/верификация на КЕП, както и Политика за употреба на удостоверение за време.

I. УСЛОВИЯ, РЕД И НАЧИН НА ИЗПОЛЗВАНЕ НА КВАЛИФИЦИРАН ПОДПИС

1. Общи правила на използване на подписа

1.1. Автор/Титуляр използва КЕП при съблюдаване на следните основни изисквания:

- строго спазване на ЗЕДЕП, наредбите по приложението му и на общоустановените в международната практика препоръки и стандарти;
- най-висока степен на съхранение/защита на частния ключ за електронно подписване от страна на Автора/Титуляря;
- спазване на условията и процедурите при генерирането на двойката ключове съгласно Наръчника, независимо дали двойката ключове се генерира при ДУУ или при Автора/Титуляря;
- спазване на условията за достъп до частния ключ - използване на парола/персонален идентификационен номер (ПИН);
- строго спазване и съблюдаване на мерките и процедурите по идентификация и автентификация на заявителя на квалифицирано удостоверение за КЕП съгласно Наръчника;
- невъзможност от последващо използване КЕП при загуба на смарт карта, при унищожаване на частния ключ за подписване, изтекъл срок на валидност или прекратяване на съответстващо удостоверение;
- публично обявени практики, процедури и политики за предоставяне на удостоверителни услуги от страна на ДУУ;
- публичен достъп, 24 часа в денонощието, 7 дни в седмицата до Публичния регистър на издадените и до CRL за КЕП и до служебните удостоверения на ДУУ чрез неговия Интернет сайт;
- съблюдаване на гаранциите и застрахователната политика на ДУУ;
- зачитане на неимуществените и имуществените права и в частност правата върху интелектуалната собственост на ДУУ и на Автора/Титуляря.

2. Правила при подписване

2.1. Преди да използва частния ключ за подписване на електронен документ, Авторът/Титулярят трябва да бъде сигурен, че съответстващото удостоверение е за КЕП, т.е. е квалифицирано и е издадено в съответствие с Политиката на това удостоверение и тази политика отговаря на потребностите на Автора/Титуляря;

2.2. Проверката на Политиката е препоръчително да се осъществява чрез сравняване с идентификатори, посочени в оригинално копие на Наръчника на ДУУ;

2.3. Политиката по издаване и поддържане на удостоверението за КЕП се идентифицира в удостоверението със следните белези:

- уникален идентификатор на Политика (Certificate Policy OID);
- уникален идентификатор за квалифицирано удостоверение;

- име на ДУУ;
- дата на издаване и влизане в сила на Политиката, което е следствие от датата на издаване и влизане в сила на Наръчника;
- приложимост спрямо конкретния тип удостоверение.

3. Начин на използване - проверени софтуерни приложения

3.1. Подписването с КЕП винаги следва да се осъществява с проверени софтуерни приложения или такива, които са сертифицирани по ЗЕУ.

3.2. В сайта на ДУУ е публикуван списък със софтуерни приложения, които са проверени и за които е установено, че са пригодни за употреба на КЕП и на съответното удостоверение, с оглед предназначението му;

3.3. В дължимата грижа на Доверяващата се страна е да провери предназначението и приложимостта на удостоверението за КЕП и софтуерните приложения, с които се създава и проверява подписа.

3.4. Подписващата страна, съответно Доверяващата/проверяваща страна, принципно използват два начина на подписване с КЕП и на проверка на подписа:

- Локален – проверено софтуерно приложение за подписване/верификация ще работи в локална система при Автора/Титуляря, като при подписване достъпва локалниq четец със смарт картата с КЕП. Този начин на работа използват широко приложимите и станали де-факто стантарт локални офис-приложения за работа с е-документи (MS Office, Adobe Acrobat, др.) или клиентски софтуерни пакети и инструменти за подписване/проверка, които се предоставят от ДУУ;
- Отдалечен – проверено софтуерно приложение за подписване/верификация работи като услуга или в сървърна система, като при подписване отдалечено достъпва четеца със смарт карта с КЕП към локалната система на Автора/Титуляря. ДУУ предоставя онлайн услуги за подписване/верификация.

4. Ограничения при употреба на подписа

4.1. КЕП има правна стойност на саморъчен подпис, ако се употребява със съпътстващо квалифицирано удостоверение за КЕП, в рамките на приложното поле на това удостоверение, както и по отношение на допълнително договорени между Автора/Титуляря и Доверяващата се страна ограничения в начина на употреба.

4.2. Ограниченията за използване на подписа по отношение на стойността на сделките, които Автора/Титулярят може да сключва посредством КЕП и на изявленията, които може да прави, са извън обхвата на Политиката, под която Удостоверяващият орган на ДУУ издава съответното удостоверение за КЕП. Ограничаването на приложението на издадените удостоверения по отношение на стойността на сделките, които Авторът/Титулярят може да сключва посредством КЕП е предмет на съгласуване между него и Доверяващата се страна.

4.3. Ограниченията за използване на КЕП по отношение предназначението му се вписват в удостоверението посредством реквизитите “Key Usage” и “Extended Key Usage”.

4.4. Използване на КЕП извън вписаните в квалифицираното удостоверението ограничения не може да ангажира по никакъв начин отговорността на ДУУ и е изцяло за сметка на Автора/Титуляря или Доверяващата се страна. В този случай КЕП, съпътстван от такова удостоверение загубва правната си стойност на квалифициран такъв.

5. Задължения на Автора и на Титуляря при подписване

5.1. При използване на КЕП Авторът/Титулярят трябва:

- да следва и спазва точно условията и процедурите в Наръчника и съответните политики и практики при използване на подписа и консумирането на други удостоверителни услуги;
- да има основни познания относно използването на електронния подпис и PKI технологиите;
- след изтичане срока на валидност на удостоверението или след спиране или прекратяване действието му да не използва частния ключ за създаване на КЕП;
- да информира всяка Доверяваща се страна относно дължимата грижа при доверяване на КЕП и съпътстващото го квалифицирано удостоверение.

6. Техническа сигурност и контрол

6.1. Подробна информация относно изискванията за съхраняване на частния ключ и за създаване на КЕП на Автор/Титуляр се съдържа в Наръчника на ДУУ.

7. Тайна на частния ключ

7.1. С оглед опазване на тайната на частния ключ Авторът/ Титулярят трябва:

- да осигури сигурна и надеждна среда при използване на двойката ключове за КЕП с оглед опазване тайната на частния ключ;
- да използва алгоритми, съобразно изискванията на НИУЕП;
- незабавно да уведоми ДУУ, в случай на компрометиране или съмнения за компрометиране на частния ключ, като поиска временно спиране или прекратяване на действието на съответното удостоверение за КЕП;
- да съхранява и защитава надеждно тайната на своя частен ключ през периода на валидност на удостоверението срещу загуба и компрометиране, в съответствие на изискванията на Наръчника на ДУУ. Всяко използване на частния ключ се приема като извършено от Автора/Титуляря действие;
- да смени предоставения му първоначален PIN-код за достъп до смарт-карта (частния ключ) преди да използва удостоверението за КЕП, в случай че квалифицираното удостоверение е издадено на B-Trust смарт карта.

8. Генериране на нова двойка ключове

8.1. ДУУ препоръчва Титулярят/Авторът да генерира нова двойка ключове при подновяване или преиздаването на удостоверение за КЕП, с оглед редуциране на риска от компрометиране на текущата двойка ключове.

9. Компрометиране на частния ключ

9.1. В случай на компрометиране на частния ключ на Автора/Титуляря, същият е задължен незабавно да уведоми ДУУ за иницииране на процедура по прекратяване на удостоверението, съгласно Наръчника на ДУУ.

10. Унищожаване на частен ключ

10.1. Автор/Титуляр унищожава частния ключ посредством:

- инициализиране (“изтриване”) на смарт картата, ако ключът се съхранява на смарт-карта;
- физическо унищожаване на носителя (смарт картата).

11. Активиране и деактивиране на частен ключ

11.1. При инициализация на B-Trust смарт карта се генерират следните кодове за достъп, които се предоставят на Автора/Титуляря: код за деблокиране на картата “Unblock PIN” и начален потребителски код за достъп „User PIN”.

11.2. Авторът е длъжен на смени началния потребителски код, посредством софтуера, който се предоставя с B-Trust смарт картата.

11.3. ДУУ препоръчва Автора да сменя периодично потребителския код за активиране на достъпа до смарт-картата.

11.4. Авторът следва надлежно да пази и да използва само при нужда предоставеният му код за деблокиране на блокирана смарт карта.

11.5. Достъпът до частния ключ за създаване на КЕП се осъществява посредством поставяне на смарт картата в карточетеца и въвеждане на PIN-кода за достъп или осъществяване на персонална идентификация по друг начин.

11.6. Частен ключ за създаване на КЕП се деактивира посредством прекратяване действието на удостоверението за този КЕП.

11.7. Ако частният ключ е записан на смарт карта, възможността за използването му се прекратява посредством изваждане на смарт картата от карточетеца.

11.8. Ако частният ключ е записан на друг носител, възможността за използването му се прекратяване посредством изваждането на носителя от компютъра и преустановяване на достъпа до ключовия файл.

11.9. Кодовете за достъп до SSCD се предават на Автора/Титуляря отделно от картата.

II. ПРИЕМАНЕ НА ПОДПИСА

1. Доверие в електронния подпис

1.1. Доверяваща се страна – адресат на подписано електронно изявление или електронен документ с КЕП на Автор/Титуляр следва да приеме и се довери, че подписът има правна стойност на саморъчен подпис спрямо нея и обвързва Автора/Титуляря, само след като положи дължимата грижа да провери всички обстоятелства относно валидността на положения електронен подпис.

2. Дължима грижа на Доверяваща се страна

2.1. Използването на КЕП предполага лицата, които се доверяват на квалифицираното удостоверение за подписа да притежават основни познания относно принципите на функционирането на B-Trust PKI инфраструктурата на ДУУ.

2.2. Доверяващата се страна следва да положи дължимата грижа като:

- се довери на удостоверението само с оглед на предназначението и условията в Политиката, съгласно която е издадено това удостоверение и отчете допълнително съгласуваните и договорирани с Автора/Титуляря ограничения при използване на КЕП в отношенията с Титуляря/Автора;
- провери в удостоверението обозначената политика, приложима към това удостоверение (“Certificate Policy”) и предназначението и ограниченията на действието на удостоверението;
- провери предназначението на подписа чрез полетата: “Key Usage”, “Extended Key Usage” и “Qualified Statement” в удостоверението. Полето “Basic constrains” трябва да бъде установено по следния начин: “Subject Type = None”. Полето “Key Usage” следва да съдържа “Non-repudiation, Digital Signature”. Полето “Qualified Statements” трябва да съдържа идентификатора ‘0.4.01862.1’;
- провери ограничението за използването на удостоверението по отношение стойността на имуществения интерес, ако има такова. В общия случай ограничението е извън обхвата на Политиката на ДУУ за квалифицирано удостоверение за КЕП и е предмет на съгласуване и договаряне между Автора/Титуляря и Доверяващата се страна. Ограничението, ако има такова, не е по отношение отговорността на Доставчика за вреди от издадено удостоверение за КЕП;
- определи дали удостоверението не е издадено за тестови демонстрационни нужди.

2.3. Доверяващата се страна следва да се увери, че издаденото удостоверение е за КЕП. Проверката се осъществява:

- на базата на вписаният OID на Политиката, под която е издадено това удостоверение от ДУУ;
- на база съдържанието в полето “Qualified Statements”;
- на база съдържанието полето “Subject”, чрез низа „Personal Certificate – UES”, съответно “Professional Certificate - UES”, ако този низ присъства.

2.4. Доверяващата се страна следва да провери формата на данните, които са подписани - за да се провери електронният подпис, е необходимо да се знае точно каква информация или обект са били подписани. Утвърдени международни препоръки, спецификации и стандарти за криптография с публични ключове задават стандартните формати на полагане на КЕП към електронно изявление или документ на Автора/Титуляря: PKCS#7, CMS, XML-DSIG, XAdES, др.

2.5. Доверяващата се страна следва да провери, че ДУУ е вписан в публикувания Регистър на КРС по ЗЕДЕП.

2.6. Доверяващата се страна следва да се увери, че Авторът е лицето, вписано в удостоверението и действа в рамките на представителната си власт по отношение на Титуляря, ако има вписан такъв.

2.7. Доверяващата се страна следва да извърши проверка на статуса на квалифицираното удостоверение в поддържания от ДУУ Публичен регистър. Проверката на автентичността и интегритета на удостоверението - т.е. подписът на ДУУ, не осигурява проверка за неговата валидност и всички настъпили вреди от предприети действия след осъществяване единствено на такава проверка, са за сметка на Доверяващата страна.

2.8. Доверяващата се страна трябва да провери, чрез проверка до приемливо ниво на доверие, например: оперативно удостоверение на ДУУ, дали удостоверението на Автора/Титуляря не е прекратено или временно спряно. Прекратяване или спиране на действието на удостоверението води като правна последица до невалидност на подписа. Проверката за валидност на статуса се осъществява чрез използване на CRL, OCSP или преглед на Регистъра на издадените удостоверения на ДУУ.

2.9. Доверяващата се страна следва да проверява/верифицира електронния подпис към електронно подписани изявления, както и да верифицира електронния подпис на ДУУ по веригата от удостоверения до приемливо ниво или до базовото удостоверение. Тази проверка следва да е базирана на стандарта X.509. Проверката за валидност на КЕП е по отношение на успешното потвърждаване валидността на удостоверенията в цялата верига, в която участва това удостоверение за КЕП. Конкретно за домейна B-Trust в тази верига участват базовото удостоверение на Удостоверяващия орган „B-Trust Root CA“ и оперативното удостоверение на Удостоверяващия орган „B-Trust Operational CA QES“.

2.10. Доверяващата се страна следва се увери, че приложенията, с които се използва удостоверението са функционално приложими за предназначението, за които е издаден, както и с оглед нивото на сигурност, посочени в съответната Политика..

2.11. Доверяващата се страна следва да се увери, че такова приемане е разумно при съответните обстоятелства. В случай, че обстоятелствата налагат необходимостта от допълнителни гаранции за доверие и увереност, Доверяващата се страна следва да положи съответна грижа за изграждане на пълното доверие и увереност.

2.12. В дължимата грижа на Доверяващата се страна е да използва механизъм за сигурна проверка на подписа, който гарантира, че:

- публичният ключ, който се използва за фактическа проверка на подписа съответства на този, която се визуализира пред него;
- проверката за използването на частния ключ е надеждно потвърдена и резултатите от тази проверка коректно се визуализират;
- доверяващото се лице може при необходимост да установи съдържанието на подписания електронен документ;

- автентичността и валидността/действителността на удостоверението към момента на подписване/употреба на КЕП са надеждно проверени;
- резултатите от проверката и електронната идентичност на Автора/Титуляря правилно се визуализират;
- всякакви промени, релевантни за сигурността са установими.

2.13. ДУУ не носи отговорност за настъпили вреди за Доверяващата се страна от неполагане на дължимата грижа.

III. УСЛОВИЯ, РЕД И НАЧИН НА ИЗПОЛЗВАНЕ НА УДОСТОВЕРЕНИЕ ЗА ВРЕМЕ

1. Общи правила

1.1. Политиката на специализирания Орган на ДУУ за УВ съдържа условията, реда и процедурите за издаване, доставка и поддържане на УВ за потребителите.

1.2. ДУУ издава УВ на всяка заинтересована страна като съблюдава стандартно/ негарантирано ниво на обслужване.

1.3. Потребител, който се нуждае от гарантирано ниво на обслужване на УВ сключва договор с ДУУ.

1.4. ДУУ издава УВ за два типа съдържание – на КЕП и на произволен електронен документ.

1.5. УВ следва да е публикувано в публичен Регистър за УВ към специализирания Орган на ДУУ.

2. Издаване на УВ

2.1. ДУУ издава УВ под обща политика с идентификатор „OID = 0.4.0.2023.1.1”.

2.2. УВ с идентификатор на политика, различна от горепосочената, се издават на потребители, които имат договор с ДУУ със съгласувано ниво на обслужване (SLA) на УВ;

3. Начин на използване на УВ

3.1. УВ с идентификатор на политика „OID = 0.4.0.2023.1.1” са приложими за употреба в приложения с различен профил:

- Употреба на КЕП към определен момент във време – УВ се интегрира към КЕП на подписания документ. Тази употреба на УВ създава ‘безотказност’ (non-repudiation) на КЕП във времето - т.е. валидността на КЕП се разширява извън периода на валидност на квалифицираното удостоверение за този КЕП. Този начин на използване на УВ позволява да се употребява разширен формат на КЕП (XAdES, CAdES, PAdES) в съответните приложения;
- Създаване на удостоверение за съдържание на електронен документ преди определен момент, т.е. удостоверение за непроменимост на съдържанието на

електронния документ след момента в УВ. Този начин на използване на УВ се прилага в изграждане на архиви, регистри, е-форми, др.;

3.2. УВ със съгласувана политика на издаване и употреба се използват в специализирани приложения на потребители на УВ.

4. Ограничаване при употреба на УВ

4.1. Политиката на ДУУ с общ идентификатор „OID = 0.4.0.2023.1.1" в УВ не ограничава приложимостта на доставяните УВ по преценка на потребителите.

4.2. УВ със съгласувана политика на издаване и употреба, включена в тези УВ обслужват само конкретните страни съгласно договора с ДУУ. ДУУ не носи отговорност, когато приложимостта на УВ е извън посочената в тях политика.

5. Задължение на страните при употреба на УВ

5.1. Задълженията и отговорностите на ДУУ при доставка и поддръжка на УВ с общ идентификатор на политика „OID = 0.4.0.2023.1.1" са дадени в документа „Политика и практика на органа за удостоверяване на време B-Trust Time Stamp Authority" на ДУУ;

5.2. Задълженията и отговорностите на ДУУ при доставка и поддръжка на УВ със съгласуван идентификатор на политика се посочват в отделен документ (SLA), неделима част от договора с ДУУ.

5.3. Потребителите на УВ следва:

- Да приемат базовото удостоверение на ДУУ, изграждащо доверието към този ДУУ и неговия специализиран Орган, доставящ УВ;
- Да използват квалифицираното удостоверение на Органа за УВ с цел проверка на КЕП в УВ;
- Да извършат проверка на КЕП като следват указанията, съгласно този документ.

5.4. Доверяваща се страна трябва да провери КЕП в УВ и валидността на удостоверението на Органа, издал УВ.

5.5. В случай, че това удостоверение е с изтекъл срок на валидност Доверяващата се страна трябва:

- Да провери в CRL за това удостоверение;
- Да провери нивото на сигурност на използваната хеш-функция съгласно Политиката;
- Да провери нивото на сигурност на алгоритмите и дължината на ключовата двойка на КЕП.

6. Техническа сигурност и контрол

6.1. Техническата сигурност и контрола при употребата на УВ са в пълно съответствие с публичния документ „Политика и практика на органа за удостоверяване на време B-Trust Time Stamp Authority " на ДУУ.

IV. Приемане на удостоверение за време

1. Доверие в УВ

1.1. Доверяваща се страна–адресат в употребата на УВ следва да се довери и да приеме, че УВ има официална удостоверителна сила спрямо нея и обвързва ДУУ, само след като положи дължимата грижа да провери всички обстоятелства относно валидността на издаденото УВ.

2. Дължима грижа на Доверяваща се страна

2.1. Доверяващата се страна следва да провери в публичния Регистър за УВ на ДУУ за УВ с този номер

2.2. Да положи дължимата грижа като следва посочените указания, описани в настоящия документ.