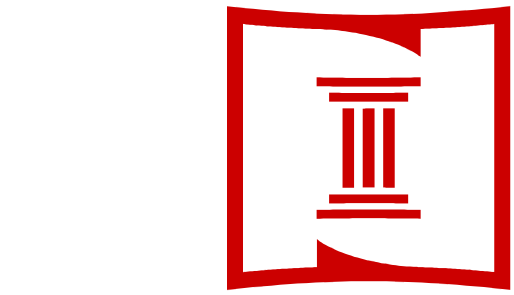

InfoNotary

ПОЛИТИКА

ЗА ПРЕДОСТАВЯНЕ
НА УДОСТОВЕРИТЕЛНИ УСЛУГИ ЗА КВАЛИФИЦИРАН
ЕЛЕКТРОНЕН ПОДПИС НА ФИЗИЧЕСКО ЛИЦЕ
ОТ ИНФОНОТАРИ ЕАД

i-Notary Personal Q Sign – Privacy Enforced CP

Версия 1.0

В сила от 26 Юли 2013 г.

ИНФОНОТАРИ ЕАД

Адрес на управление: ул.”Иван Вазов” № 16, ет.6, 1000 София, България,
ЕИК:131276827

III. ПОЛИТИКА ЗА ПРЕДОСТАВЯНЕ НА УДОСТОВЕРИТЕЛНИ УСЛУГИ ЗА КВАЛИФИЦИРАН ЕЛЕКТРОНЕН ПОДПИС

(1) “Политиката за предоставяне на удостоверителни услуги за квалифициран електронен подпис” е документ, неделима част от Наръчника за потребителя, описващ политиката и процедурите, които Доставчикът следва при издаване на удостоверения, както и приложимостта на издаваните удостоверения с оглед сигурността на тези процедури.

(2) За всички типове удостоверения, които издава, Доставчикът разработва и съблюдава различна удостоверителна политика.

(3) Удостоверителната политика за тип удостоверение включва правилата, по които се извършват първоначалната идентификация и автентификация на Титулярите и Авторите на удостоверения за електронен подпис, както и политиката за управление на издадените удостоверения – спиране, възобновяване и прекратяване действието на издадено от Доставчика удостоверение.

(4) Удостоверителната политика на всеки тип удостоверение определя и ограниченията в приложимостта на удостоверенията в зависимост от нивото на сигурност при проверките и степента на доверие в удостоверените в издадения документ факти.

(5) Удостоверителните политики на удостоверенията за квалифициран електронен подпис съдържат и условията и реда за използване на квалифицирания електронен подпис и изискванията за съхраняване на частния ключ.

I.1. Политика за издаване и управление на Удостоверение за квалифициран електронен подпис на Физическо лице със защита на лични данни

I.1.1. Обща характеристика на удостоверението

(1) Удостоверението i-Notary Personal Q Sign Certificate - Privacy Enforced има характер на удостоверение за квалифициран електронен подпис по смисъла на чл. 16, т.1 от ЗЕДЕП и всеки електронен подпис, който е придружен от това удостоверение, има характера на квалифициран електронен подпис. В това удостоверение са ограничени личните данни, които са вписани за идентификация на Авторите и Титулярите.

(2) Удостоверение за квалифициран електронен подпис на Физическо лице със защита на личните данни (i-Notary Personal Q Sign Certificate - Privacy Enforced) се издава на физическо лице – Титуляр и Автор, и удостоверява идентичността и връзката с публичния му ключ.

(3) Удостоверението i-Notary Personal Q Sign се издава задължително с генерирани и съхранявани в криптографско устройство (смарт карта) двойка криптографски ключове – частен и публичен, ползвани за създаване и проверка на квалифициран електронен подпис.

(4) За издаване на удостоверението i-Notary Personal Q Sign Certificate - Privacy Enforced се прилагат процедури, осигуряващи високо ниво на надеждност и сигурност на удостоверената информация, идентифицираща Титуляря и Автора и държането на средствата за създаване на електронен подпис – частния ключ.

(5) При процедурите за идентификация и установяване на самоличността на Титуляря и на Автора се изисква представяне на доказателства за самоличността на Титуляря, самоличността на Автора, както и за представителната власт на Автора и личното им явяване пред Регистриращ орган на Доставчика.

I.1.2. Предназначение и приложимост на удостоверението

(1) Удостоверението i-Notary Personal Q Sign Certificate - Privacy Enforced може да бъде ползвано като средство за персонална електронна идентификация при електронна търговия, финансови транзакции, електронна кореспонденция, електронно подписване на документи, извършване на изявления от и до държавни органи и органи на местното самоуправление по смисъла на ЗЕДЕП.

(2) В дължимата грижа на Доверяващата се страна е да провери предназначението и приложимостта на това удостоверение, когато се доверява на електронния подпис, който удостоверението придружава.

(3) За проверката от Доверяващата се страна в удостоверението се обозначават политиката, приложима към това удостоверение ("Certificate Policy"), и допълнителните разширения към нея и предназначението и ограниченията на действието на удостоверението, описани в Атрибутите "Key Usage", "Extended Key Usage","Qualified Statements".

I.1.3. Обозначение

(1) Политиката, приложима към това удостоверение, се обозначава по следния начин:

	Вид политика	Наименование	Обозначение (OID)
	Удостоверителна политика за Удостоверение за квалифициран електронен подпис на физическо лице със защита на личните данни	i-Notary Personal Q Sign Certificate - Privacy Enforced CP	1.3.6.1.4.1.22144.1.1.1.3

(2) Политиката е публикувана в Публичния документен регистър на Доставчика и е достъпна на адрес:

http://repository.infonotary.com/certpolicy_qsign_personal_pe.html

I.1.4. Профил на удостоверението Personal Q Sign Certificate-PE

Основни x509 атрибути:

Атрибут	Стойност
Версия	3 (0x02)
Сериен номер	Уникален в регистъра на Доставчика; 8-байтово число
Начало на периода на валидност	Датата и часът на подписване на УЕП
Край на периода на валидност	Датата и часът на подписване на УЕП + от 1 до 3 календарни години
Алгоритъм на електронния подпис върху УЕП	FIPS DSS; dsaWithSHA1 (1.3.14.3.2.27) или RSA – 2048 бита

Атрибути на издателя (x509 Issuer DN)

Атрибут	OID	M[1]	T/A[2]	Стойност
/commonName	2.5.4.3	+	A	
/countryName	2.5.4.6	+	A	
/postalCode	2.5.4.17		T	
/localityName	2.5.4.7		T	
/unstructuredAddress	2.5.4.9	+	T	
/organizationName	2.5.4.10	+	T	
/organizationalUnitName	2.5.4.11			-
/emailAddress	1.2.840.113549.1.9.1		A	
/telephoneNumber	2.5.4.20		T	

[1] Задължителен (Mandatory)
[2] Титуляр/Автор

Допълнително дефинирани атрибути на организация				
/bgEIK/BULSTATNumber	2.5.4.10.100.1.1			-
/bgTaxationNumber	2.5.4.10.100.1.2			-
/bgBankAddressableUnit	2.5.4.11.100.1.2			-
/bgBudgetIdentificationNumber	2.5.4.11.100.1.1			-
/bgLegalRegistration	2.5.4.10.100.1.3			-
Допълнително дефинирани атрибути на физическо лице				
/bgUnifiedCitizenNumber	2.5.4.3.100.1.1	+	T	
/bgIdentificationCardNumber	2.5.4.3.100.1.2		T	
/bgFinancialObligationsStatement	2.5.4.3.100.1.3		T	
/bgRepresentativeDocumentNumber	2.5.4.3.100.1.4			-

Атрибути на Титуляря/Автора (x509 Subject DN):

Атрибут	OID	M[3]	T/A[4]	Стойност
/commonName	2.5.4.3	+	A	
/countryName	2.5.4.6	+	A	
/emailAddress	1.2.840.113549.1.9.1		A	
Допълнително дефинирани атрибути на физическо лице				
/bgFinancialObligationsStatement	2.5.4.3.100.1.3		T	

Атрибути на Автора (x509v3 subjectAltName extension DN):

Атрибут	OID	M	T/A	Стойност
/commonName	2.5.4.3			-

[3] Задължителен (Mandatory)
[4] Титуляр/Автор

/countryName	2.5.4.6	+	A	
/emailAddress	1.2.840.113549.1.9.1			-
Допълнително дефинирани атрибути на физическо лице				
/bgFinancialObligationsStatement	2.5.4.3.100.1.3			-
/bgRepresentativeDocumentNumber	2.5.4.3.100.1.4	+	A	

Допълнителни x509 атрибути (x509v3 extensions):

Атрибут	OID	M	C[5]	Стойност
/basicConstraints	2.5.29.19	+	+	CA=false
/keyUsage	2.5.29.15	+	+	NonRepudiation,DigitalSignature
/extKeyUsage	2.5.29.37	+		emailProtection, clientAuth
/authorityKeyIdentifier	2.5.29.35			subjectKeyIdentifier на подписващото УЕП
/subjectKeyIdentifier	2.5.29.14	+		SHA1 от DER - кодирания публичен ключ
/cRLDistributionPoints	2.5.29.25	+		http://crl.infonotary.com/crl/qsign-personal-ca.crl ldap://ldap.infonotary.com/dc=qsign-personal-ca,dc=infonotary,dc=com
/authorityInfoAccess	1.3.6.1.5.5.7.1.1	+		http://ocsp.infonotary.com/responder.cgi
/qcStatements	1.3.6.1.5.5.7.1.3			0.4.0.1862.1.1

CertificatePolicies x509v3 extension:

Идентификатор (OID)	1.3.6.1.4.1.22144.0
CPS	http://www.crc.bg
Текст	Registration Resolution № .....by the Communication Regulation Commission

[5] Критично (Critical)

Идентификатор (OID)	1.3.6.1.4.1.22144.1.1.1.1
CPS	http://repository.infonotary.com/certpolicy_qsign_personal_pe.html
Текст	InfoNotary personal qualified certificate

Идентификатор (OID)	0.4.0.1456.1.1
CPS	http://www.infonotary.com/qcp-sscd.html
Текст	This certificate is issued as qualified certificate for advanced electronic signature using secure storage cryptographic device

Описание и приложение на атрибутивните OID, използвани в RDN на Удостоверението

Описание на атрибутите

Атрибут	OID	P[6]	Значение
/commonName	2.5.4.3		Име на субекта
/countryName	2.5.4.6		Код на държавата
/emailAddress	1.2.840.113549.1.9.1		e-mail адрес
/telephoneNumber	2.5.4.20		Телефонен номер
/bg/EIK/BulstatNumber	2.5.4.10.100.1.1	+	ЕИК/БУЛСТАТ
/bgTaxationNumber	2.5.4.10.100.1.2	+	Данъчен номер на организацията
/bgFinancialObligationsStatement	2.5.4.3.100.1.3	+	Финансови ограничения на сделките, подписвани с УЕП
/bgRepresentativeDocumentNumber	2.5.4.3.100.1.4	+	Информация за номера и издателя на документа за представителство

Описание на формата и формирането на атрибутите

Атрибут	Формат	S[7]	Pr[8]	Източник

[6]Собствен (Дефиниран от Доставчика като разширение на съществуващ X.500 атрибут)
[7]Разделител
[8]Префикс

/commonName	A+	,		Трите имена на Автора/Титуляря
/countryName	A2			Двусимволен код на държава
/postalCode	N4			Пощенски код
/localityName	AN+			Град
/unstructuredAddress	AN+	,		Данните от адреса
/emailAddress	IA5+			e-mail адрес на Автора
/telephoneNumber	AN+			Телефонен номер на Титуляря/Автора
/bgEIK/BULSTATNumber	N+		BULSTAT:	БУЛСТАТ/ЕИК номер
/bgTaxationNumber	N+		TAXNUM:	Данъчен номер
/bgBankAddressableUnit	N+		BAU:	Банкова адресируема единица
/bgBudgetIdentificationNumber	N+		BIN:	Бюджетен идентификационен номер
/bgLegalRegistration	AN+	,	LEGAL:	Информация за търговската или друга регистрация на организация
/bgIdentificationCardNumber	N+		IDCARD:	Номер на личната карта/паспорт
/bgFinancialObligationsStatement	AN+	:	FO:	Минимална стойност, максимална стойност и ISO код на валута на ограничението
/bgRepresentativeDocumentNumber	AN+		REPDN:	Информация за номера и издателя на документа за представителство

Колоната "Формат" има следното значение:

Формат	Значение
A	Атрибутът може да приема само буквени стойности
N	Атрибутът може да приема само цифрови стойности
AN	Атрибутът може да приема буквено-цифрени стойности
IA5	Атрибутът може да приема валидни IA5 символи (e-mail/url)

- *Числото след обозначението на формата обозначава максимален брой допустими символи.*

- *Символът ” + “ обозначава един или повече символа.*
- *Всяко поле, освен маркираните като IA5, съдържа данни в UTF-8 кодиране.*
- *Датите в полетата за валидност са представени като ASN1 GeneralTime*

I.1.5. Процедура по заявяване издаването на удостоверението

(1) Регистриращите органи на Доставчика приемат и обслужват всички искания за издаване на удостоверения за квалифициран електронен подпис от крайни потребители.

(2) Искане за издаване на удостоверение до Доставчика могат да отправят всички лица, които:

- попълнят Искане за издаване на удостоверение;
- генерират двойка криптографски ключове, самостоятелно или посредством Доставчика;
- предоставят на Удостоверяващия орган на Доставчика публичния ключ, кореспондиращ на частния ключ;
- приемат условията на Договора за предоставяне на удостоверителни услуги и Наръчника за потребителя на Доставчика.

(3) Искането за издаване на удостоверение е необходимо да съдържа следните данни:

- информация, индивидуализираща Титуляря, и ако Авторът е различен от Титуляря, и информация за Автора;
- публичния ключ, кореспондиращ на частния ключ от двойката криптографски ключове, генерирани от Титуляря;
- типа на избраното удостоверение.

(4) Искането за издаване на удостоверение е електронен документ във формат PKCS #10, подписан с частния ключ, кореспондиращ на публичния, включен в документа.

(5) Искането за издаване на удостоверение се подава лично от Заявителя в Регистриращ орган на Доставчика или може да бъде създадено през интернет портала на Доставчика и отправено към него

посредством криптиран комуникационен канал на адрес: https://www.infonotary.com.

(6) Регистриращите органи на Доставчика предоставят услуга на всички лица по генериране на двойката криптографски ключове, създаване на искане за издаване на удостоверение и представянето им пред Доставчика.

(7) Когато Регистриращият орган на Доставчика извършва по искане от Титуляря генериране на двойка криптографски ключове, ползва защитен механизъм за създаването им и ги предоставя на Автора, записани на крипографско защитено устройство – смарт карта или др.

(8) Правата за достъп до частния ключ – ПИН код или парола, се предоставят от Регистриращия орган на Автора в защитен вид.

(9) След предаването от Регистриращия орган на устройството (SSCD), на което е записан частният ключ и правата за достъп до него, Титулярят и Авторът носят пълната отговорност за предотвратяване на компрометиране, загуба, разкриване, модифициране или друго неоторизирано използване на техния частен ключ.

I.1.6. Потвърждаване или отхвърляне на заявките за удостоверения

(1) За установяване и потвърждаване на самоличността на физическо лице, направило искане за издаване на удостоверение, се прилагат процедури и спазват правила, определени от Доставчика.

(2) Проверките и потвърждаването на информацията се извършват от Регистриращия орган съобразно правилата за и процедурите на Доставчика и в пълно съответствие с Наръчника за потребителя и други вътрешни документи.

(3) Регистриращият орган проверява и потвърждава следната информация, идентифицираща Физическото лице – Титуляр, Автор или упълномощен представител на Титуляра:

- лично, бащино и фамилно име;
- дата на раждане;
- място на раждане;
- националност;

- пол;
- адрес, град, държава, пощенски код;
- Единен граждански номер (ЕГН);
- номер на документ за самоличност: лична карта, паспорт;
- издател, дата на издаване и валидност на документа за самоличност;
- представителната власт на Автора и/или Представителя;
- информация за контакти и фактуриране.

(4) Титулярят, Авторът или упълномощения представител на Титуляря представят лично пред Регистриращия орган следните документи:

- валиден документ за самоличност: лична карта или паспорт;
- нотариално заверено пълномощно за упълномощаване на Представителя да представлява Титуляря/Автора пред Доставчика за издаване и управление на удостоверения;
- документ, доказващ представителната власт на Автора – съдебно решение, удостоверение за актуално състояние, нотариално заверено пълномощно или друг овластяващ акт.

(5) Преди потвърждаване на подадено искане за издаване на удостоверение Регистриращият орган на Доставчика извършва необходимите проверки, като:

- проверява и потвърждава самоличността или идентичността на Заявителя, Автора, Титуляря или представляващото го лице по предоставените от тях документи;
- проверява и потвърждава представителната власт на Автора и упълномощеното от Титуляря да го представлява лице;
- проверява коректността на получената или направената подписана електронна заявка (във формат PKCS#10) за издаване на удостоверение;
- предоставя на Титуляря или Автора информацията, която е потвърдена и ще бъде включена в издаденото удостоверение за приемане на съдържанието му.

- събира необходимите документи за удостоверяване на извършените проверки (копия на представените от Титуляря, Автора или Упълномощения представител документи, саморъчно заверени с дата и подпис от лицата).

(6) След направените проверки и приемане на съдържанието на удостоверението от Титуляря или Автора Регистриращият орган потвърждава искането за издаване на удостоверение към Удостоверяващия орган на Доставчика и гарантира, че:

- искането за издаване изхожда от Титуляря или от надлежно овластено от него лице или от Автора;
- информацията относно Титуляря и Автора, представена за включване в удостоверението, е вярна и пълна;
- частният ключ е технически годен да бъде използван за създаване на усъвършенстван електронен подпис и съответства на публичния ключ, така че чрез публичния ключ може да се удостовери, че определен електронен подпис е създаден с частния ключ, и
- частният ключ се държи от Автора.

(7) Ако процесът на потвърждаване на заявката за издаване на удостоверение завърши неуспешно, Регистриращият орган отхвърля искането за издаване на удостоверение.

(8) Регистриращият орган незабавно уведомява Заявителя и посочва причината за отхвърлянето директно или посредством:

- изпращане на електронно писмо до Титуляра, респективно Автора и
- лично, на място в Регистриращия орган

(9) Заявители, чиито искания за издаване на удостоверение са били отхвърлени, могат отново да подадат искане за издаване на удостоверение.

(10) Регистриращият орган окомплектова и съхранява предоставените от Титуляря, Автора и Заявителя документи (заверени копия или оригинали) заедно с искането за издаване на удостоверение,

протокола за приемане на удостоверението и подписан договор за удостоверителни услуги.

(11) Доставчикът контролира точността на включената в удостоверението информация, предоставена на Титуляря и Автора към момента на издаване на удостоверението.

(12) Проверката и потвърждаването на информацията в направените искания за издаване на удостоверения се обработват в разумен срок и Доставчикът издава удостоверенията до 5 работни дни от датата на приемане на документите.

I.1.7. Издаване на Удостоверението

(1) Удостоверяващият орган на Доставчика издава удостоверението на база на получено искане за издаване от Регистриращия орган.

(2) Искането за издаване на удостоверение от Регистриращия орган гарантира потвърждаването на валидността на заявката, направена от Заявителя, валидността на данните, съдържащи се в нея, и е подписано от администратора на Регистриращия орган, извършил проверките.

(3) Удостоверяващият орган на Доставчика проверява идентичността на Регистриращия орган и самоличността на администратора на Регистриращия орган на база на представени пълномощия (специално административно удостоверение на администратор на Регистриращ орган).

(4) След издаване на удостоверението Доставчикът го доставя до Титуляря, съответно до Автора:

- чрез вписване на връзка за дънлоуд на удостоверението в изпратеното електронно писмо ;
- или посредством записването му на смарт картата (SSCD) от Регистриращия орган.

I.1.8. Приемане на удостоверението

(1) Доставчикът издава удостоверението в съответствие със съгласието на Титуляря, респ. Автора.

(2) Приемане на съдържанието на удостоверението се удостоверява с подписване на Протокол за приемане на удостоверение за квалифициран електронен подпис от Титуляря, респ. Автора преди публикуването му в Регистъра на удостоверенията на Доставчика.

I.1.9. Публикуване на удостоверението от Удостоверяващия орган

Доставчикът публикува незабавно издаденото удостоверение за квалифициран електронен подпис в Регистъра на удостоверенията си.

I.1.10. Спиране и възобновяване на удостоверението

Спирането и възобновяването на удостоверението се извършва по общите процедури за Спиране на удостоверения и Възобновяване на удостоверения съгласно т. 4.9.11 и т. 4.9.16 от Наръчника за потребителя.

I.1.11. Прекратяване на удостоверението

Прекратяването на удостоверението се извършва по общите процедури за Прекратяване на удостоверения съгласно т. 4.9 от Наръчника за потребителя.

I.1.12. Подновяване на удостоверението

Подновяване на удостоверението се извършва по общите процедури за Подновяване на удостоверения съгласно т. 4.6 от Наръчника за потребителя.