



РЕПУБЛИКА БЪЛГАРИЯ

АПЕЛАТИВЕН СЪД – ВЕЛИКО ТЪРНОВО

ОДОБРИЛ:
Хр. Даскалова
и.ф. Председател на
Апелативен съд –
Велико Търново

Hristina
Konstanti
nova
Daskalova

Digitally signed
by Hristina
Konstantinova
Daskalova
Date: 2026.10.19
15:24:51 +03'00'

Ръководство за проверка и подписване на електронни документи

В България квалифицирани електронни подписи (КУКЕП) могат да издават само доставчици на квалифицирани удостоверителни услуги, вписани в националния доверителен списък на КРС. [\[crc.bg\]](https://crc.bg)

Към момента вписани доставчици са:

- Борика АД (услугата **B-Trust**)
- Евротръст Технолъджис АД (**Evrotrust**)
- Инфонотари ЕАД (**InfoNotary**)
- Информационно обслужване АД (**StampIT**)
- „Идокс България“ ЕООД

1. Проверка за валидност на електронно подписани документи.

При приемане на електронно подписани документи следва да се провери валидността на квалифицирания електронен подпис (КЕП), самоличността на подписващото лице и целостта на документа. Необходимо е да се установи, че подписът е издаден от квалифициран доставчик на удостоверителни услуги и че към момента на подписване сертификатът е бил валиден. Проверката се извършва в съответствие с Регламент (ЕС) № 910/2014 (eIDAS) и приложимите технически спецификации ETSI EN 319 102-1 и ETSI EN 319 102-2 за валидиране на електронни подписи и удостоверителни вериги.

1.1.Методика за проверка:

- Проверка на валидността на КЕП чрез специализиран софтуер или онлайн валидатор.



РЕПУБЛИКА БЪЛГАРИЯ

АПЕЛАТИВЕН СЪД – ВЕЛИКО ТЪРНОВО

- Проверка на статуса на сертификата (валиден, отнет, спрян или изтекъл).
- Проверка на удостоверителната верига до квалифициран доставчик на удостоверителни услуги и наличието на доверие към издателя на сертификата.
- Проверка дали сертификатът е бил валиден към момента на подписване на документа.
- Проверка на времевия печат, когато е наличен.
- Проверка за използване на криптографски алгоритми и параметри, отговарящи на действащите изисквания за сигурност.
- Проверка за промени в документа след подписването и потвърждаване на целостта на подписаните данни.
- Проверка на криптографската валидност на електронния подпис.
- Установяване на съответствие между данните на подписващото лице и данните, съдържащи се в сертификата.
- Проверка дали подписът е квалифициран електронен подпис, издаден въз основа на квалифициран сертификат.
- Документиране на резултата от валидирането, включително установените предупреждения, ограничения или грешки.

1.2. Валидатори.

Почти всички оторизирани доставчици на удостоверителни услуги предлагат собствен ресурс за проверка на валидност на електронно подписани документи. Едни са уеб базирани, а други е необходимо да инсталирате като приложен софтуер. На посочените по-долу адреси може да направите бърза справка за валидността на електронно подписан документ.

- [Evrotrust DSS Validation Service](#)
- [B-TRUST | Qualified Signature Validation Service](#)
- [InfoNotary Validation Services](#)
- [DSS Demonstration WebApp \(НАРЕДБА ЗА УДОСТОВЕРЕНИЯТА ЗА ЕЛЕКТРОНЕН ПОДПИС В АДМИНИСТРАЦИИТЕ ЧЛ.27 Т.6\)](#)



РЕПУБЛИКА БЪЛГАРИЯ

АПЕЛАТИВЕН СЪД – ВЕЛИКО ТЪРНОВО

2. Електронно подписване на документ.

2.1. КЕП с физически носител.

При този вариант квалифицираният сертификат и частният ключ се съхраняват върху защитен хардуерен носител, например смарт карта или USB токен. Подписването се извършва локално на компютъра на потребителя и обикновено изисква включване на устройството и въвеждане на ПИН код.

В зависимост от формата на документа най-често използваните стандарти за подписване са PAdES, CAdES . Съществуват други стандарти за формат на подписване като XAdES, JAdES, CB-AdES, но няма да бъдат разглеждани в това ръководство.

Стандартът **PAdES** се използва за подписване на PDF файлове. Това е универсален файлов формат за пренасяне на документи и е препоръчителен от множество организации поради съвместимостта и лесната работа с него . Съществува огромно разнообразие от приложен софтуер за подписване на електронни документи. Пример за такива софтуерни пакети са разработени от самите доставчици на удостоверителни услуги, както и разработки на трети страни спазващи изискванията на eIDAS.

CAdES представлява стандарт за електронно подписване, базиран на Cryptographic Message Syntax (CMS/PKCS#7), предназначен за създаване и валидиране на усъвършенствани и квалифицирани електронни подписи съгласно Регламент (ЕС) № 910/2014 (eIDAS). Файлове могат да бъдат от произволен формат и съдържание: както текстови формати, така и изображения и други електронни файлове. Съществуват два формата на пакетиране при CAdES: Enveloping/Attached CAdES – създава се файл с разширение .p7m, съдържащ едновременно оригиналния документ и електронния подпис. Detached CAdES – създава се файл с разширение .p7s, съдържащ единствено електронния подпис, като оригиналният файл се съхранява отделно. CAdES се използва основно за подписване на файлове от произволен тип, обмен на електронни документи между информационни системи и дългосрочно съхранение на електронни подписи съгласно приложимите европейски технически стандарти.



РЕПУБЛИКА БЪЛГАРИЯ

АПЕЛАТИВЕН СЪД – ВЕЛИКО ТЪРНОВО

Тук може да намерите кратък списък с уеб базирани услуги и приложен софтуер, необходим за подписване на електронни документи.

Софтуер, предоставени от доставчика на удостоверителни услуги.

- **InfoNotary** – [eDoc signer](#)
- **Btrust** - [Подписване на файлове ON-LINE](#) + [BISS](#)
- **Btrust** - [Desktop Signer](#)
- **Информационно обслужване** – [DS tool](#)
- **Информационно обслужване** - [Подписване на файл :: sign.uslugi.io](#)

Други софтуерни продукти отговарящи на стандартите за електронно подписване.

- [Adobe Acrobat Reader](#) – приложение за настолен компютър
- [Digital Signature Service Application](#) (DSSA) - приложение за настолен компютър
- Други приложни софтуери

2.2.Облачен (cloud-based) КЕП.

При облачния КЕП частният ключ не се намира при потребителя, а се съхранява в защитена инфраструктура на доставчика на удостоверителни услуги, която отговаря на изискванията за квалифицирано устройство за създаване на подпис (QSCD). Подписването се потвърждава чрез допълнителна идентификация, например мобилно приложение, SMS код или друго средство за двуфакторна автентикация.

3. Препратки и кратки ръководства с инструкции за подписване и валидиране на документи:

- 3.1.[Инструкция за подписване на документи с квалифициран електронен подпис в InfoNotary e-Doc Signer – Infonotary](#)
- 3.2.[Инструкция за инсталация и работа с приложението B-Trust Desktop Signer](#)

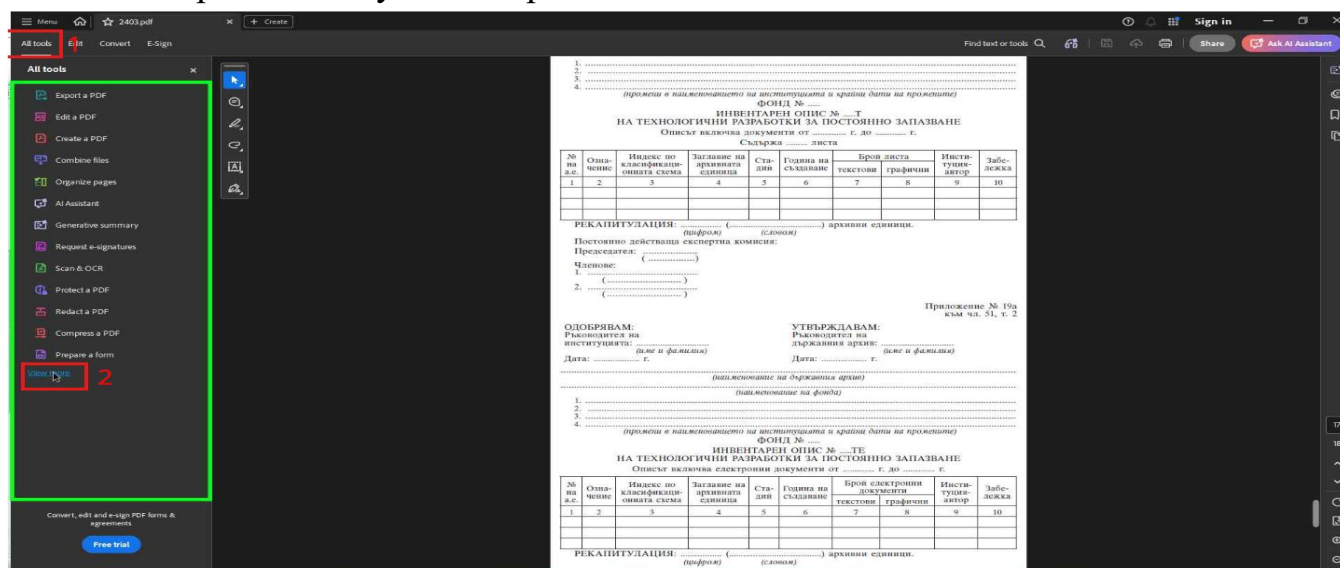


РЕПУБЛИКА БЪЛГАРИЯ

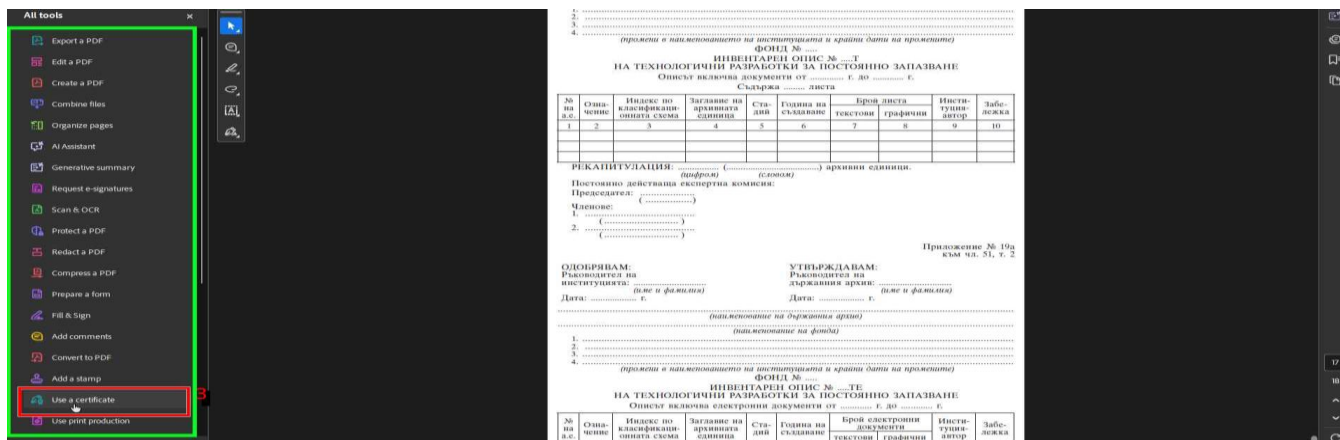
АПЕЛАТИВЕН СЪД – ВЕЛИКО ТЪРНОВО

3.3.Инструкция за подписване с приложно програмнен продукт Acrobat Reader.

(Избирате 1:All tools -> 2:View more->3:Use certificate-> 4:Digitally sign -> 5:Описвате правоъгълник като задържите десния бутон на мишката където ще бъде положен електронния подпис в документа -> 6:Избирате КЕП с вашите имена от диалоговия прозорец -> 7: Continue -> 8: Sign->Save->“Екранна снимка 7“:Показва се диалогов прозорец за въвеждане на ПИН към електронния ви подпис. След което процесът за подписване на електронния документ е приключил.



Екранна снимка 1

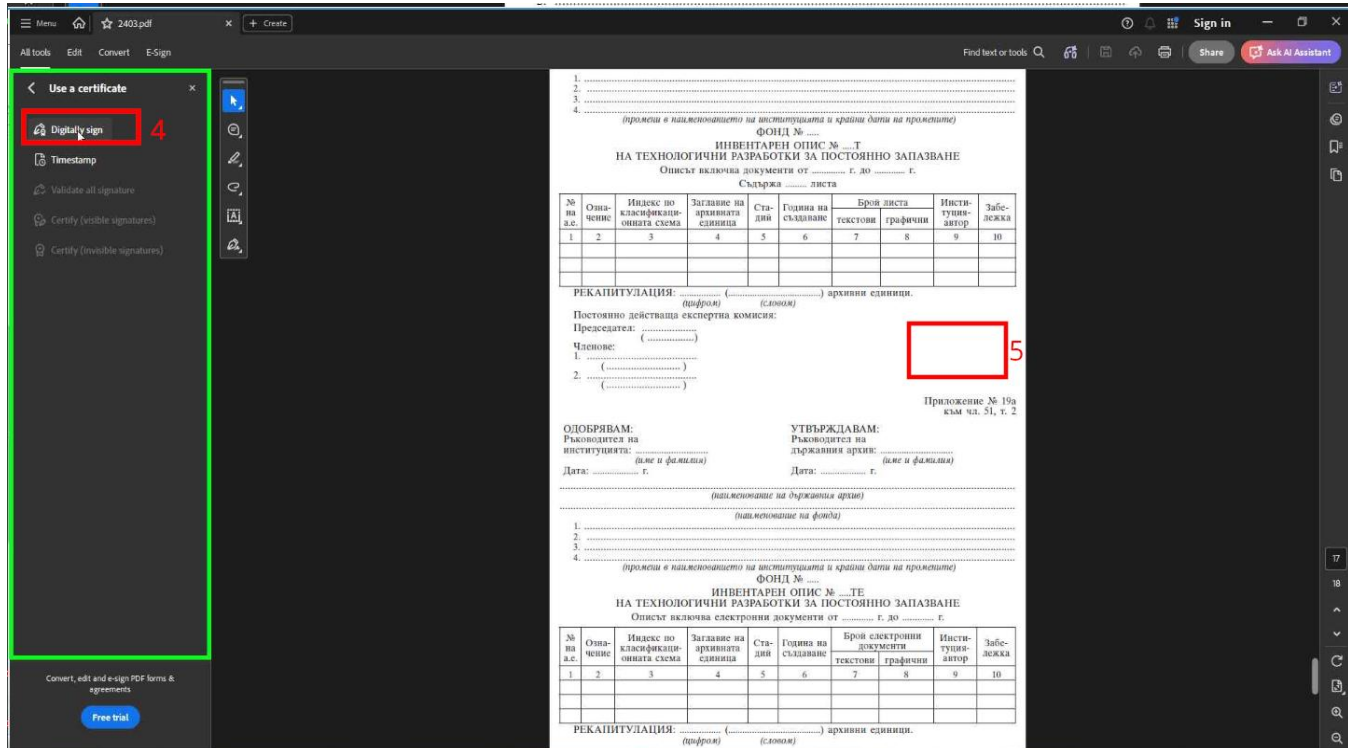


Екранна снимка 2



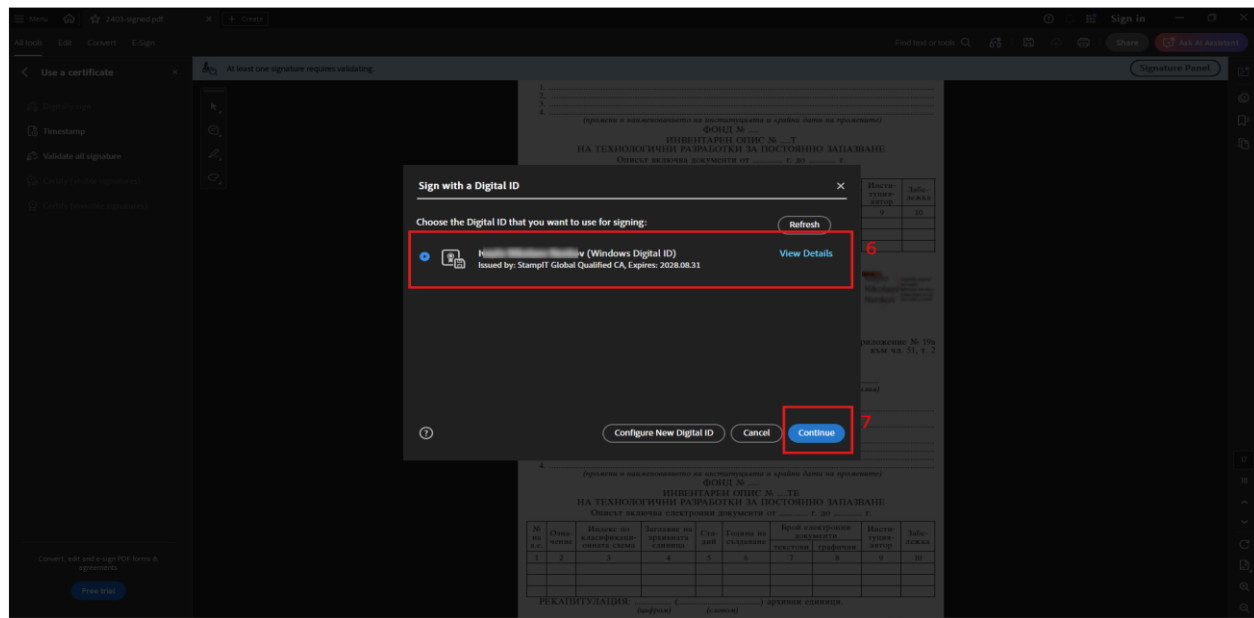
РЕПУБЛИКА БЪЛГАРИЯ

АПЕЛАТИВЕН СЪД – ВЕЛИКО ТЪРНОВО



Екранна снимка 3

В екранна снимка 4 може да изберете вашия сертификат, с който желаете да подпишете файла.

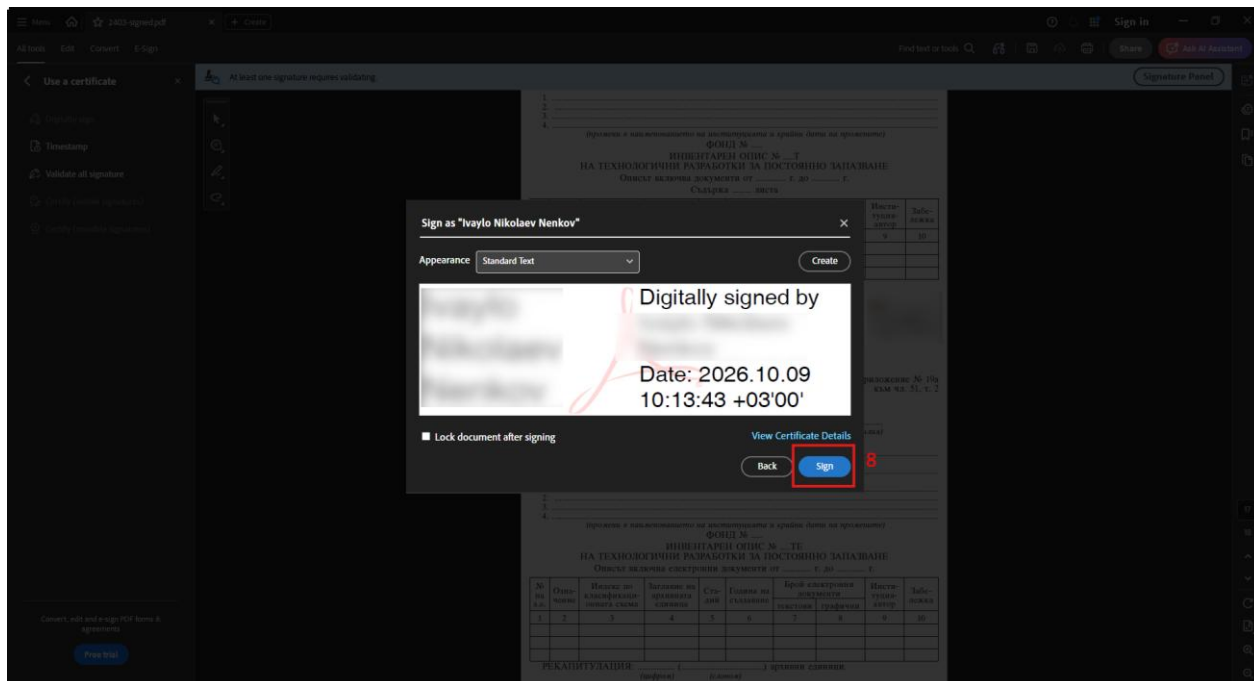


Екранна снимка 4



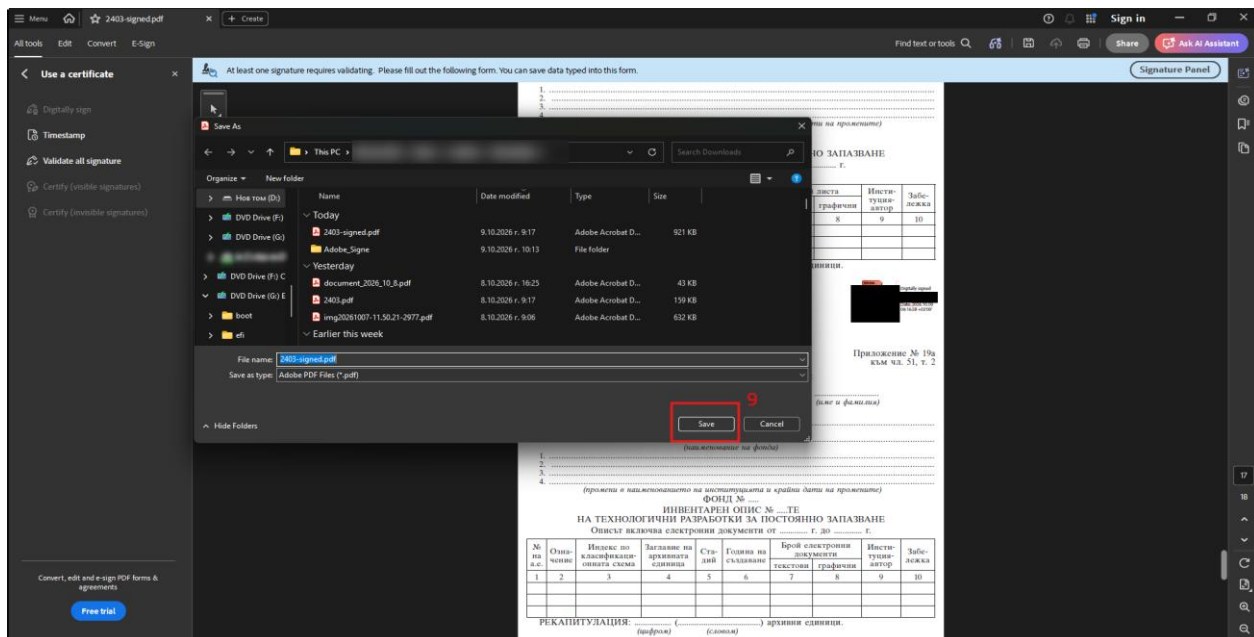
РЕПУБЛИКА БЪЛГАРИЯ

АПЕЛАТИВЕН СЪД – ВЕЛИКО ТЪРНОВО



Екранна снимка 5

Ако желаете може да преименувате файла. По подразбиране се презаписва върху съдържанието на неподписания файл

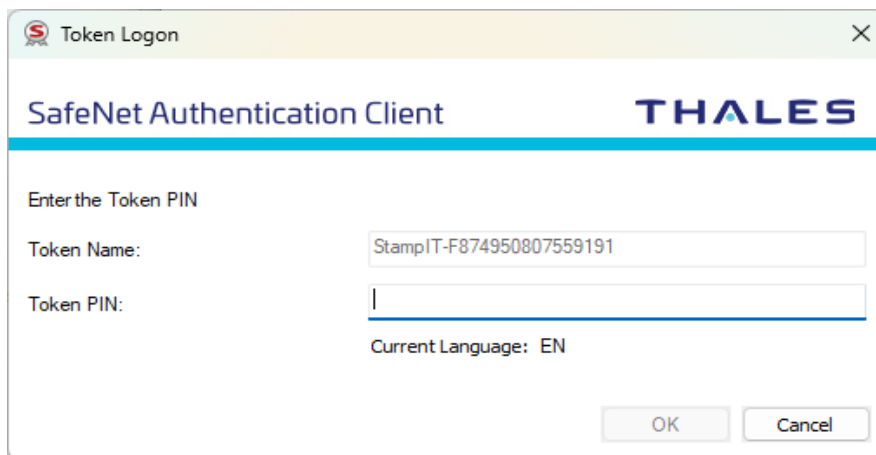


Екранна снимка 6



РЕПУБЛИКА БЪЛГАРИЯ

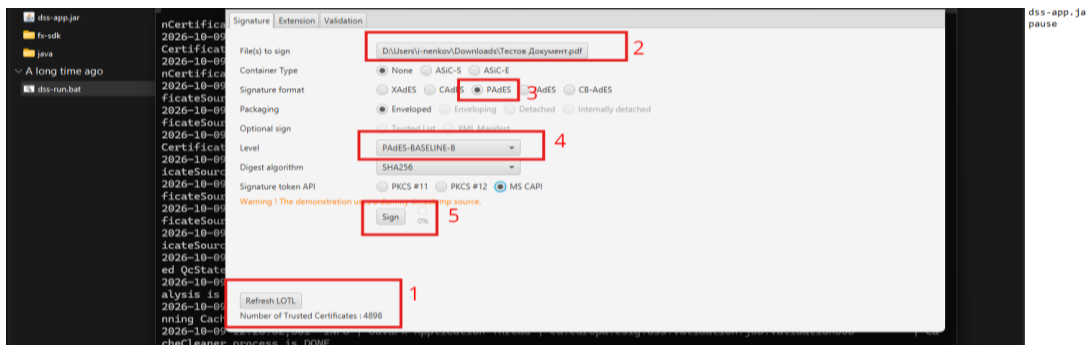
АПЕЛАТИВЕН СЪД – ВЕЛИКО ТЪРНОВО



Екранна снимка 7

3.4. Пример за подписване с приложение DSSA.

След като изтеглите и разархивирате приложението се стартира от dss-gui->1:В следващата стъпка се зарежда интерфейсът на приложението. Трябва да обновим LOTL списъците с доверените сертификати-> Избирате документа който трябва да се подпише -> 3:Посочваме формата (за PDF – PadES, ако е друг формат изберете CAdES). 4: Избирате нивото на подписване (разработеното приложение работи единствено с –B(ase) ниво), ако желаете променете дайджест алгоритамът, **но не избирайте SHA1!** SHA-1 не отговаря на съвременните изисквания и не се смята за сигурен.5: Натискате бутона “sign”-> Показва се диалогов прозорец за избор на сертификат -> Въвежда се ПИН на сертификата -> 7: Избира се име на файл и се запазва.

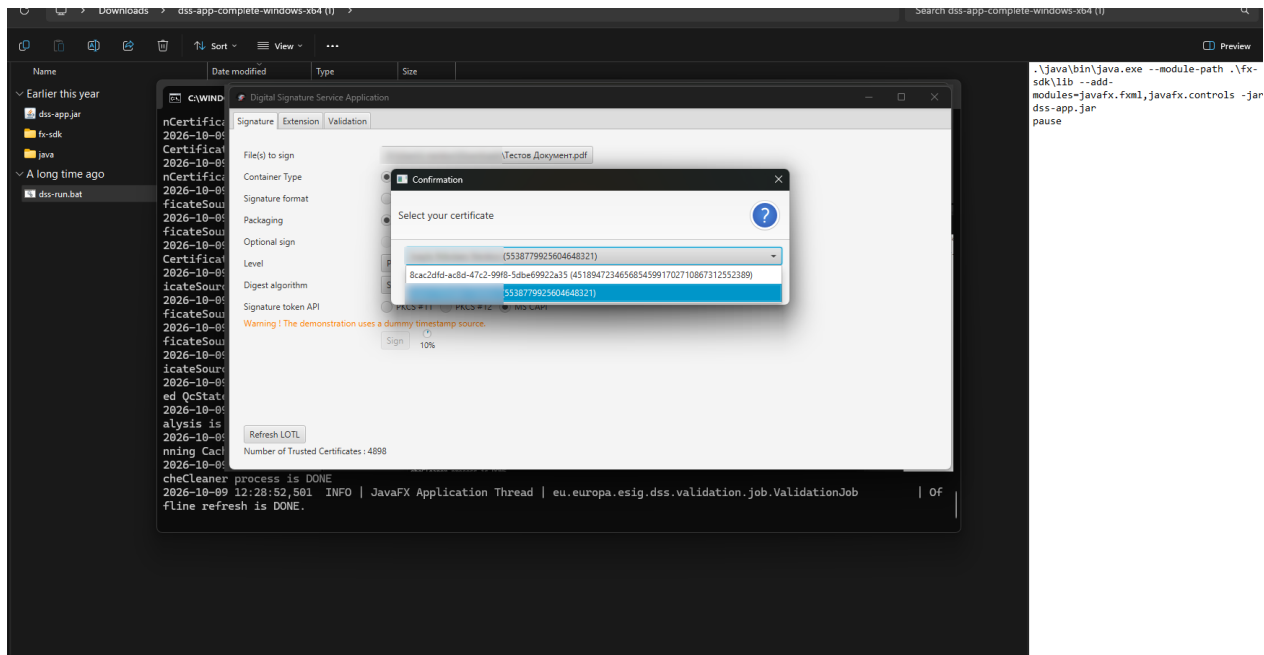


Екранна снимка 8

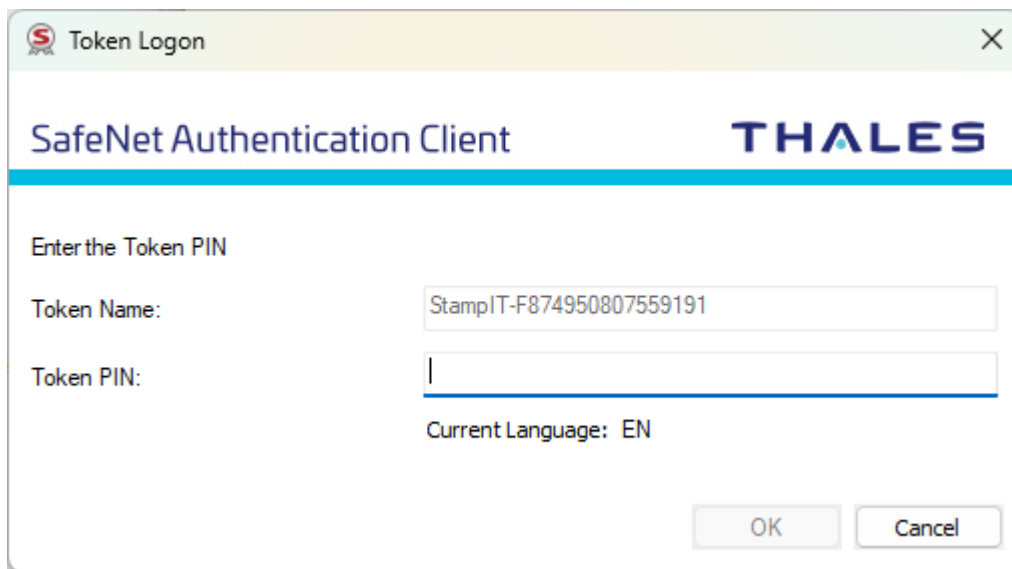


РЕПУБЛИКА БЪЛГАРИЯ

АПЕЛАТИВЕН СЪД – ВЕЛИКО ТЪРНОВО



Екранна снимка 9

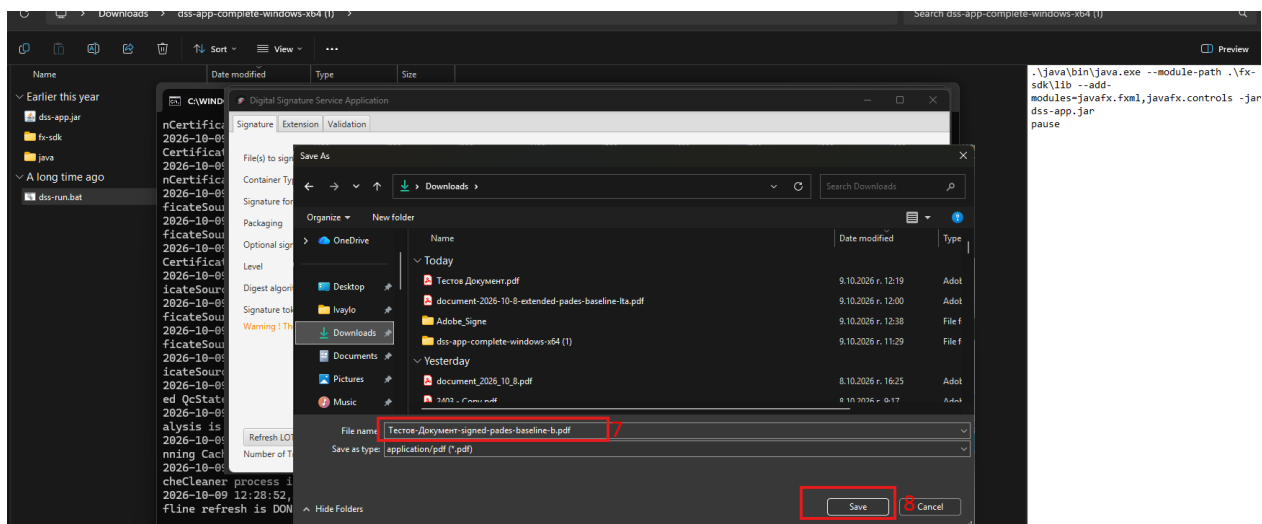


Екранна снимка 10



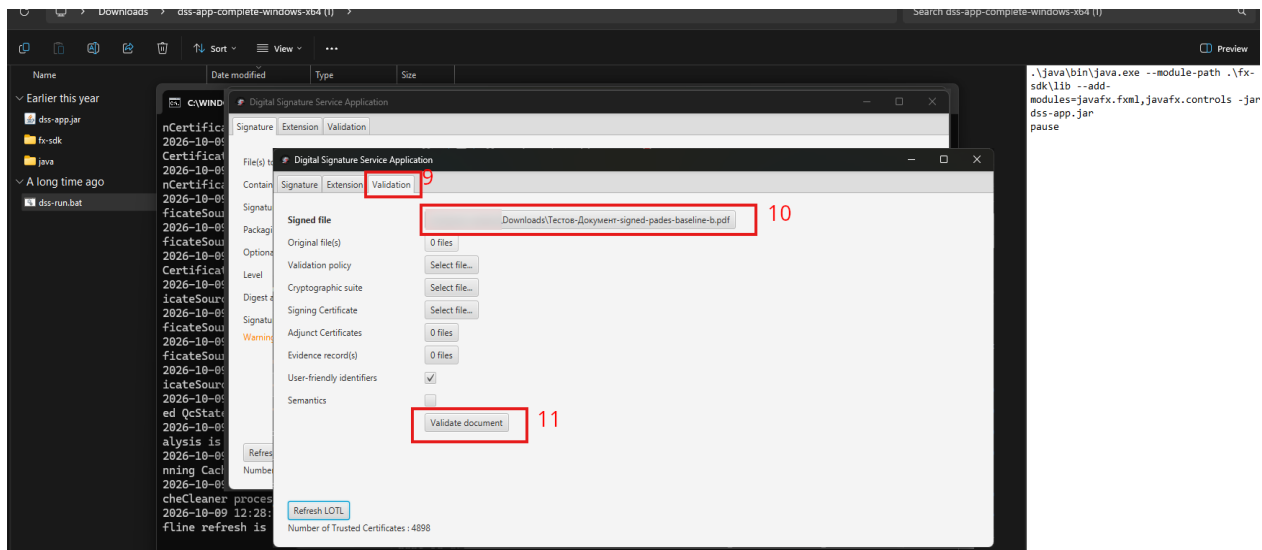
РЕПУБЛИКА БЪЛГАРИЯ

АПЕЛАТИВЕН СЪД – ВЕЛИКО ТЪРНОВО



Екранна снимка 11

След стъпка 8, процесът по подписване на електронния документ е приключил. Ако желаете може да проверите (валидирате) подписания файл. Това не е задължителна процедура. След като се опреснят LOTL – списъците с доверените сертификационни вериги избираме таб 9: validation->10: избираме файла който трябва да проверим ->11: Натискаме бутона “Validate document” и на екрана се визуализира резултата от проверката „Екранна снимка 13“



Екранна снимка 12

