# Услуга за електронно подписване на документи „B-Trust Signing Service”

**Какво представлява „B-Trust Signing Service”?**

„**B-Trust Signing Service**” е **комерсиална услуга**, която осигурява възможност да се извършва подписване, валидиране, криптиране и декриптиране на електронни документи посредством използване на удостоверения за електронен подпис, включително за Квалифициран електронен подпис ( КЕП).

**За кого е предназначена услугата?**

Услугата е удобна за Клиенти, които имат необходимост от електронно подписване, валидиране, криптиране или декриптиране на голямо количество документи и нямат възможност да инсталират и поддържат при тях съответното сигурно устройство за създаване на подписи ( SSCD ).

**Какво отличава „B-Trust Signing Service”?**

Основни предимства на услугата са:

- *Високо бързодействие*: Посредством използването на съвременни Hardware Security Module SSCD се постига съответната по-висока производителност на системите, осигуряващи криптографските операции;
- *Надеждност* – системата е надеждно осигурена и обезпечава работоспособността на услугата за продължителен период от време без прекъсване;
- *Защита на информацията* – посредством изградения криптиран канал се осигурява защита на обменяната информация между Клиента и B-Trust;
- *Ниво на обслужване* – предлага се необходимото ниво на обслужване ( Service Level Agreement ), което дава възможност за бързо и навременно отстраняване на възникналите проблеми при Клиента;
- *Удостоверяване на време* на електронно подписаните документи;
- Възможност за изграждане на електронно подписани документи, които *могат сами да се валидират* - с цел дълготрайно съхранение;
- Поддръжка на *различни формати на електронно подписани документи*.

**Техническа реализация**

Услугата работи с различни формати и типове подписани документи и предлага възможност за вграждането в тях на удостоверение за време, удостоверение за статус и други атрибути.

Услугата работи върху сървърите на B-Trust като Web Service, който се достъпва чрез използването на криптиран канал за връзка ( VPN). При използване на удостоверение за КЕП, частният ключ на удостоверението се генерира, съхранява и използва в сигурно устройство за създаване на подписа (SSCD) от тип Hardware Security Module (HSM). Достъпът до него се държи от Автора на удостоверението за КЕП.

*Поддържат се следните файлови формати:*

- PKCS7 - позволява подписване на произволни документи (attached и detached)
- PDF (attached)
- XML – XadES – само за XML (attached), Open XAdES - контейнер за подписване на произволни документи (attached и detached)