




Enostavna, hitra, varna in zakonsko skladna uvedba digitalnega podpisa v vašo aplikacijo!

SETCCE proXSign® je zbirka naprednih programskih gradnikov za digitalno podpisovanje, šifriranje in časovno žigosanje na osnovi infrastrukture javnih ključev (PKI). Programske knjižnice nudijo enostavno, hitro, varno in zakonsko skladno integracijo v poljubno spletno ali namizno aplikacijo.

SETCCE proXSign® v2.1 je podprta v naslednjih operacijskih sistemih in brskalnikih (za spletne aplikacije):

Operacijski sistemi	Spletni brskalniki
<p>Windows </p> <ul style="list-style-type: none"> XP⁽¹⁾,7,8,8.1,10 	<ul style="list-style-type: none"> Internet Explorer od v8 do v11 Edge od v20 Mozilla Firefox od v30 Google Chrome od v55 Opera od v42 Safari v5.1.7
<p>MAC OS X/macOS </p> <ul style="list-style-type: none"> Yosemite 10.10 El Capitan 10.11 Sierra 10.12 	<ul style="list-style-type: none"> Safari 9.0.1 in 9.0.3 Safari 10.0.1 (Sierra 10.12) Mozilla Firefox od v52 Google Chrome od v57
<p>Linux </p> <p>Uradno podprte distribucije⁽²⁾:</p> <ul style="list-style-type: none"> Ubuntu 16.10 (amd64) Ubuntu 16.04 (amd64) Fedora 24 (x86_64) Fedora 25 (x86_64) <p>Komponenta je na voljo tudi za nekatere druge Linux distribucije, vendar ni uradno podprta: glej Linux distribucije.</p>	<ul style="list-style-type: none"> Mozilla Firefox – glej priporočila za posamezno Linux distribucijo Google Chrome od v55
<p>Opombe:</p> <p>(1) Minimalne zahteve: Windows XP Service Pack 3.</p> <p>(2) Zadnji dve uradno razpoložljivi različici na dan 24.1.2017.</p>	



Standardi

Komponenta SETCCE proXSign® v2.1 je skladna z naslednjimi standardi:

- W3C XMLDsig
- W3C XMLEnc
- ETSI XAdES-BES, eSLOG/XAdES, ETSI XAdES-T, ETSI PAdES-BES
- Adobe PDF (ISO/IEC 32000-1:2008)
- PDF/A
- Je odjemalec strežnika za časovno žigovanje po XAdES-T ali Entrust XML shemi

SETCCE proXSign® v2.1 sledi smernicam uredbe (EU) No 910/2014 (eIDAS).

Lastnosti in glavne funkcionalnosti

Glavne lastnosti in funkcionalnosti komponente SETCCE proXSign® v2.1:

- Podpora za operacijske sisteme **Windows, Mac in Linux** in **vse najbolj popularne brskalnike**.
- **Enostavna namestitvev** in en/enoten namestitveni paket za vse brskalnike.
- Podpora za **tiho namestitvev** (WIN).
- **Samodejna posodobitev** komponente (WIN).
- **Enostavna integracija:** enoten javascript vmesnik za vse platforme in brskalnike.
- **Sočasna uporaba različnih shramb digitalnih potrdil:**
 - ✓ Windows in Mozilla Firefox (NSS) shrambe digitalnih potrdil na WIN OS.
 - ✓ Keychain in Mozilla Firefox (NSS) shrambe digitalnih potrdil na MAC OS X / macOS.
 - ✓ Mozilla Firefox in Google Chrome/Chromium (NSS) shrambe digitalnih potrdil na (LINUX).
- Podpora za digitalna potrdila, ki se nahajajo na zunanjih medijih (pametne kartice/USB ključi) ali ki so nameščena v shrambe digitalnih potrdil oz. brskalnike (»soft« digitalna potrdila)
- Skladnost s standardi: **XMLDsig, XAdES-BES, eSLOG/XAdES, Adobe (PKCS#7), PDF/A, PAdES-BES, XML Entrust** shema za časovno žigovanje, **XAdES-T**, na osnovi **PKI** (X.509 digitalna potrdila).
- Digitalno podpisovanje PDF dokumentov do formata **PDF 1.7**.
- Podpora za **SHA1, SHA2** (SHA-256, SHA-384, SHA-512) kriptografske zgoščevalne algoritme.
- Nekatere funkcionalnosti, zaradi omejitev Mac Cripto knjižnic, na MAC OS X/macOS niso na voljo (osebna digitalna potrdila so nameščena v shrambi digitalnih potrdil Keychain):
 - ✓ OS X Yosemite (10.10): SHA2 (SHA-256, SHA-384, SHA-512) kriptografski zgoščevalni algoritmi in PAdES.
 - ✓ OS X El Capitan (10.11) in macOS Sierra (10.12): SHA-384, SHA-512 kriptografski zgoščevalni algoritmi in PAdES.
- **Na OS X/macOS so vse funkcionalnosti podprte preko Mozilla Firefox shrambe digitalnih potrdil (NSS).**
- Podpora za **RSA/DSA** podpisne kriptografske algoritme.
- Tipi podpisov: **Enveloped, Enveloping, Detached** (XMLDsig).
- **XML/PDF preverjanje veljavnosti podpisa** (XML preverjanje podpisa po XMLDsig).

- **Preverjanje digitalnega potrdila** (časovna veljavnost, preverba verige digitalnih potrdil, preverjanje preklica digitalnih potrdil (CRL)).
- Hkratno podpisovanje več dokumentov.
- **Podprti vhodni formati dokumentov:**
 - ✓ XML niz (poljuben tip podpisa)
 - ✓ Vgrajena binarna datoteka v base64 formatu (enveloping podpis)
 - ✓ Zunanja XML datoteka (poljuben tip podpisa)
 - ✓ Zunanja binarna datoteka (detached podpis)
- **Konfigurabilnost:**
 - ✓ Več podpisov istega dokumenta (zaporedni podpis).
 - ✓ Podpisovanje poljubnih delov (deli XML dokumenta, celoten dokument, etc).
 - ✓ Izbira digitalnega potrdila po splošnem imenu (CN), razločevalnem imenu (DN), izdajatelju (issuer), serijski številki (serial number), prstnem odtisu (hash).
 - ✓ Poljubno nastavljen vizualni prikaz digitalnega podpisa na PDF dokumentu: vodni žig (slika) in poljubno pozicioniranje le-tega glede na stran (pozicijo se določi s koordinatami).
- **Šifriranje** poljubnega XML niza ali XML datoteke in **dešifriranje**.
- **Časovno žigosanje** (po XAdES-T ali Entrust XML shemi)
- Podpora za **večjezičnost**.
- **Vrsta primerov uporabe** za hitro in lažjo integracijo.
- **On-line testno orodje**.
- Potrjena tehnološka ustreznost (glej www.w3.org/Signature).

OPOMBA:

- Nekatero funkcionalnosti, kot so SHA-2 zgoščevalni algoritmi in šifriranje pri uporabi digitalnih potrdil na zunanjih medijih (pametna kartica/pametni USB ključ) morda niso na voljo. Podpora je odvisna od gonilnikov in kriptografskih knjižnic, ki jih uporabljajo zunanji mediji.
- Podpora za digitalna potrdila na zunanjih medijih (pametne kartice/USB ključi).
 - So podprta, če jih podpirata Windows ali Keychain shrambi digitalnih potrdil.
 - Podpora standarda PKCS#11 bo na voljo v eni od bodočih izdaj komponent SETCCE proXSign®.

SETCCE proXSign® SDK paket

SETCCE proXSign® SDK paket za razvijalce vsebuje:

- **proXSign® v2.1 WEB komponente** (za spletne aplikacije)
 - ✓ proXSign komponente za podprte operacijske sisteme
 - ✓ proXSign JavaScript knjižnice
 - ✓ Primere uporabe
 - ✓ Navodila za integracijo komponent
 - ✓ Navodila za končne uporabnike
 - ✓ Pomožna orodja
- **proXSign® v2.1 COM komponento** za namizne aplikacije (komponenta ni vključena v SETCCE proXSign® SDK paket, za informacije pišite na info@proxsign.com).

Za informacije o ostalih podpisnih komponentah ali za dodatna vprašanja smo vam na voljo na info@proxsign.com.