

Instrucțiuni pentru obținerea certificatului digital in ierarhie privată

Înainte de a începe procedura de înregistrare pentru obținerea certificatului digital trebuie să vă descărcați și să vă instalați utilitarele și driverele pentru dispozitivul securizat de creare a semnăturii, aflate pe site-ul nostru, la opțiunea **Produse si Servicii** în secțiunea **Aladdin eToken PRO**. Acest lucru trebuie făcut înainte de a conecta dispozitivul la calculatorul dumneavoastră. După instalarea driverelor, trebuie să restartați calculatorul și să conectați dispozitivul la calculator. În acest moment sistemul de operare va recunoaște dispozitivul și îl va instala.



Prima pagina | Site Map

Despre noi	Produse si servicii	Portofoliu	Parteneri	Contact
----------------------------	-------------------------------------	----------------------------	---------------------------	-------------------------

[Prima pagina](#) > [Produse si Servicii](#) > Aladdin eToken PRO

Aladdin eToken PRO

Utilitare


- Driver E-Token Aladdin
- Utilitare E-Token Aladdin

1. [Prezentare](#)
2. [Caracteristici](#)
3. [Avantaje](#)
4. [Aplicatii](#)
5. [Aplicatii software suportate](#)
6. [Specificatii tehnice](#)

EToken PRO asigura autentificare si non-repudiere pentru aplicatii precum eBanking, tranzactii bursiere, eCommerce si tranzactii financiare.

Operatiunile integrate de RSA 1024-bit si 2048-bit ale eToken PRO permit integrarea in arhitecturile Infrastructurii Cheii Publice (PKI). eToken PRO genereaza si stocheaza chei private, parole si certificate digitale in insusi mediul protejat al chip-ului sau. Cheia privata a utilizatorului ramane in permanenta pe token.

Efficient ca si cost si usor de folosit, eToken PRO este un adevarat smartcard fara cititor ce poate fi mutat cu usurinta de la un calculator la altul, poate fi purtat pe breloc sau in buzunar.



Folosind tehnologie avansata de criptare, eToken PRO ofera atat autentificare realizata de catre doi factori cat si autentificare realizata prin doua metode. Avand integrate procesoare criptografice avansate, certificare de securitate ITSEC nivel 4 si carcasa protectoare rezistenta la apa si la loviri accidentale, eToken este alegerea cea mai buna pentru nevoile securitatii eBusiness.

Alte resurse

Documentatie

- Obținerea și ridicarea unui certificat digital in ierarhie publica
- Utilizarea unei semnături digitale
- Configurarea opțiunilor pentru verificarea validității certificatelor digitale in ierarhie publica pentru Acrobat Reader
- Obținerea și instalarea unui certificat de server pentru IIS
- Configurarea opțiunilor pentru autentificare pe server utilizand certificatele digitale
- Obținerea și instalarea unui certificat de server pentru Apache
- Configurarea opțiunilor pentru autentificare pe server Apache utilizand certificatele digitale

Intrebari si raspunsuri

- Forum
- Lista cu intrebari frecvente

După ce ați instalat DSCS-ul (dispozitivul securizat de creare a semnăturii - e-token), pentru a vă înregistra în vederea obținerii certificatului, accesați secțiunea **Certificate calificate din Produse și servicii**. Dacă sunteți de acord cu termenii prezenți, la pasul următor se va deschide pagina principală a centrului de eliberare a certificatelor digitale.

DigiSign Prima pagina | Site Map

Despre noi | Produse si servicii | Portofoliu | Parteneri | Contact

Prima pagina > Produse si Servicii

Produse si Servicii

.. Certificate digitale

- **Certificate calificate >>**
Sunt eliberate de Autoritatea de Certificare DigiSign S.A., permit semnarea, autentificarea si recunoasterea legala a documentelor transmise electronic, controleaza automat accesul la intranet-ul si extranet-ul dumneavoastra, protejeaza datele, asigurand securitatea tranzactiilor si protejeaza e-mail-ul prin criptare si semnaturi electronice, dovedind integritatea mesajelor.
- **Certificate server 128 biti >>**
Certificatele Global Server permit criptarea SSL pe 128 biti. - **cea mai puternica din lume** - pentru ambele versiuni de browser-e Microsoft si Netscape, devenind standard pentru comerul on line, banci, burse, organizatii de sanatate, asigurari - si orice afacere pentru care securitatea on line este o preocupare continua.
- **Certificate server 40 biti >>**
Certificatele de Server VeriSign aplica tehnologia de top SSL (Secure Sockets Layer) pentru criptarea tranzactiilor on line, permitand utilizarea unui protocol standard de securizare a comunicatiilor de pe web, iar impreuna cu Sigiliul de Securizare afisat pe web-site, conectat direct la certificatul dumneavoastra, cand vizitatorii dau click pe Sigiliu, sunt directionati pe loc catre un tablou cu informatii, asigurandu-i ca tranzactiile pe site-ul dumneavoastra sunt criptate si le dau posibilitatea sa verifice identitatea site-ului in timp real.

Oferte speciale
OFERTA

Alte resurse
Documentatie

- Obtinerea si ridicarea unui certificat digital in ierarhie publica
- Utilizarea unei semnaturi digitale
- Configurarea optiunilor pentru verificarea validitatii certificatelor digitale in ierarhie publica pentru Acrobat Reader
- Obtinerea si instalarea unui certificat de server pentru IIS
- Configurarea optiunilor pentru autentificare pe server utilizand certificatele digitale
- Obtinerea si instalarea unui certificat de server pentru Apache

Pentru începerea procesului de înregistrare apăsați pe legătura **Produse si servicii**, apoi veți fi transferat pe pagina în care vă prezentăm pașii necesari înregistrării și instalării unui certificat digital precum și actele necesare obținerii acestuia.

Pentru recunoașterea certificatului digital de către browser și sistemul de operare, trebuie să vă instalați certificatele Digisign. Menționăm că certificatele Digisign au fost testate pe browserul Internet Explorer si se recomandă folosirea versiunii 6.0 sau o versiune superioară acesteia.

În cazul în care certificatul este solicitat și obținut așa cum s-a indicat mai sus, certificatele Digisign ce trebuiesc instalate se pot obține din cadrul acestui site (**Descarcă lanț de încredere**). Apăsați butonul **Open** pentru instalarea directă a certificatului sau **Save** pentru a vă descărca și salva certificatul respectiv pe calculatorul dumneavoastră. Dacă ați apăsat butonul **Open** vă apare fereastra de instalare a certificatului: Apăsați butonul **Install Certificate...** și urmați pașii indicați (folosind butonul **Next** și lăsând opțiunile implicite în procesul de instalare). Mesajul de mai sus vă anunță că importul s-a efectuat cu succes. *Notă: În cazul în care descărcați și salvați certificatele pe calculator, făcând dublu click pe acesta va apare fereastra de instalare a certificatului.*

Dacă acceptați termenii prezentați apăsați pe link-ul **Sunt de acord**. Procesul de înregistrare va continua din acest moment pe pagina securizată. În cazul în care nu sunteți de acord cu termenii prezentați, sistemul vă întoarce pe pagina principală.

Pentru a începe procesul de înregistrare apăsați legătura **INREGISTRARE**.
Notă: *Asigurați-vă că ați conectat dispozitivul securizat la calculator.*

Formularul de înregistrare cuprinde o parte privind datele necesare înregistrării și cealaltă parte privind datele de identificare personală.

Veți completa cu atenție și cu date exacte câmpurile de pe formular. Câmpurile marcate cu * vor apărea pe certificatul dumneavoastră digital. În partea privind datele de identificare personală, pentru cetățenii români, este obligatorie completarea tuturor câmpurilor referitoare la buletin/carte de identitate și adresă. În cazul cetățenilor străini este obligatorie completarea câmpurilor referitoare la pașaport și adresă. Datele introduse în formularul de înregistrare trebuie să coincidă cu cele din declarația autenticată la notar.

Parola de acces este necesară dacă doriți să revocați certificatul digital în cazul în care cheia privată este compromisă. După ce ați completat toate datele de pe formularul de înregistrare apăsați butonul **Accept** pentru a trimite cererea dumneavoastră.

Va apărea o fereastră în care vi se solicită codul PIN al eToken-ului (în mod implicit el este 1234567890 și poate fi modificat ulterior folosind utilitarul de pe opțiunea UTILITARE). După introducerea codului PIN al eToken-ului apăsați OK.

În finalul procesului de înregistrare vă apare o fereastră prin care sunteți anunțat că înregistrarea s-a efectuat și veți primi ulterior mesaje prin e-mail privind instrucțiunile de ridicare și instalare a certificatului.

Veți primi două mesaje e-mail, unul de confirmare a cererii și altul în care sunteți anunțat dacă certificatul dumneavoastră a fost procesat. În ultimul mesaj de e-mail veți primi un cod PIN de ridicare a certificatului digital și link-ul de unde puteți face acest lucru. De pe pagina securizată a site-ului, alegeți opțiunea **Ridicarea certificatului digital**.

Veți intra pe o pagină în care sunt prezentați pașii ce trebuie urmați pentru ridicarea certificatului. În câmpul de pe această pagină introduceți codul PIN primit prin mesajul e-mail, apoi apăsați butonul **TRIMITE**. Înainte de a apăsa acest buton să vă asigurați că aveți dispozitivul securizat atașat calculatorului (cititorul de smartcard cu smartcardul introdus în cititor sau eToken-ul).

Dacă DSCS-ul folosit este smartcard va apare o fereastră în care vi se cere codul PIN al smartcard-ului (implicit el este 12345678 dar se poate modifica ulterior cu ajutorul utilitarului pus la dispoziție pe meniul UTILITARE).

Apăsați Ok și așteptați până când certificatul este inscripționat pe smartcard.

Atenție: Pentru a putea ridica certificatul trebuie să aveți setate în browser (Internet options \ Security\ Custom level) opțiunile de la *ActiveX controls and plug-ins* pe *Enabled* sau *Prompt*.

Dacă DSCS-ul folosit este e-Token inscripționarea certificatului se va face fără mesaje de atenționare. În acest moment procesul de ridicare și instalare a certificatului s-a încheiat.

Pentru a putea folosi certificatul și pe alte calculatoare decât cel de pe care s-a făcut ridicarea lui e necesar să vă instalați drivere-ele și interfața pentru DSCS-ul, certificatele autorității de certificare (în cazul nostru certificatele Digisign) cât și certificatul digital (cheia publică) aflat pe DSCS-ul (smartcard) utilizat.

Puteți verifica dacă cheia publică a certificatului s-a importat. Deschideți browser-ul, alegeți de pe meniul Tools opțiunea Internet Options. Aici selectați tab-ul Contents și apăsați butonul Certificates. În fereastra respectivă vă apar toate certificatele disponibile.