EIDCard.DLL kirjeldus

Versioon 1.0.2.1
Kuupäev: 25.11.2005

Muudatused

1.0.2.1 – 25.08.2005 – lisatud sertifikaadivaliku dialoog. Juhul, kui sertifikaadihoidlas on rohkem kui sertifikaat, mille privaatvõti on kasutatav, kuvatakse inglise keelset sertifikaadi valiku dialoogi.

1.0.1.8 – 04.09.2003 – parandatud viga, mis tõttu ei toiminud hästi setec kaardid.

1.0.1.7 – 05.06.2003 – lisatud toetus kaardile GemSAFE GPK16000. Kui võtmekonteinerite loendamine ei õnnestu (CSP ei toeta), siis kasutatakse vaikimisi võtmekonteinerit, eelnevalt kontrollides, et vaikimisi võtmekonteineriga seotud sertifikaadiga on võimalik digitaalset allkirja anda.

1.0.1.6—23.04.2003 – esimene avalik versioon

Eesmärk

EIDCard.DLL on ActiveX COM moodul, mis on mõeldud kasutamiseks veebilehtedel ID-kaardiga (EID-kaardiga) signeerimise toimingu teostamiseks. Moodul on mõeldud kasutamiseks ainult Internet Exploreriga, teiste brauserite puhul tuleks kasutada analoogilist Java signeerimise appletit.

Installimine

EIDCard mooduli kasutamiseks tuleb veebilehele lisada järgmine osa:

```
<OBJECT id=ISign codebase="EIDCard.cab#Version=1,0,2,1"
classid=clsid:FC5B7BD2-584A-4153-92D7-4C5840E4BC28></OBJECT>
```

või käivitada käsurealt:

```
regsvr32 EidCard.dll
```

Visual Basicus vms keskkonnas kasutamiseks:

```
Set ISign= CreateObject("EIDCard.Sign")
```

Kustutamine (mahainstallimine)

EIDCard mooduli kustutamiseks süsteemist tuleb teha süsteemikataloogis käsurealt:

```
regsvr32 EIDCard.dll /u
```

EIDCard.DLL kirjeldus

Meetodid

EIDCard moodul koosneb järgmistest meetoditest ja attribuutidest:

Meetod	Sisukirjeldus
String getInfo()	Väljastab info mooduli versiooni kohta: Näiteks: *EIDCard Sign Module 1.0.1.6 version 23-Apr-2003*
String getSigningCertificate()	Väljastab allkirjastamisel kasutatud sertifikaadi HEX kujul. Muudab allpool toodud atribuutide väärtusi.
String getSignedHash*(String hash, long SelectedCertNumber)*	Väljastab allkirjastatud räsi. Sisendis: *String hash* – allkirjastatav räsi *long SelectedcertNumber* – 0, kui soovitakse uuesti leida võtmekonteiner,vastasel juhul kasutatakse eelnevalt leitud (näiteks meetodiga getSigningCertificate) atribuudiga SigningKeyContainerName määratud võtmekonteinerit. Kui antud võtmekonteiner pole kättesaadav, siis leitakse uuesti kaardil oleva võtmekonteineri nimi.

Atribuudid

Atribuut	Sisukirjeldus
long selectedCertNumber	Valitud sertifikaadi number. Väärtustatakse meetodi getSigningCertificate tulemusel. Näitab sertifikaadi järjekorranumbrit sertifikaadihoidlas (Esimene sertifikaat hoidlas on järjekorranumbriga 0). Seda atribuuti kasutatakse meetodi getSignedHash ühe sisendparameetrina.

Piirangud. Teadaolevad probleemid

- Allkirjastada saab ainult kiipkaardil olevate võtmetega
- Moodul toetab ühte kaarti korraga, st kui arvuti külge on ühendatud rohkem kui 1 kaardilugeja, siis toimetab kaardiga, mille CSP nimi on tähestikujärjekorras esimesena.
- Moodul veateateid ei väljasta. Kui midagi ebaõnnestub, siis meetodite väljund on väärtustatud NULL väärtusega.
- Allkirjastamisel kasutatud sertifikaadiga seotud salajane võti võib-olla AT_KEYEXCHANGE või AT_SIGNATURE tüüpi võtmekonteineris.
- Allkirjastamisel kasutatav sertifikaat peab olema ajaliselt kehtiv ning sertifikaadi võtme kasutusala (*key usage*) peab sisaldama lippu "non-repudiation".
- Moodul on testitud järgmiste kiipkaartidega:
    - Eesti ID-kaart

    - Gemplus GemSAFE GPK8000
    - Setec SetCOS 4.3.1/2 Instant WEB card
- Moodul on testitud järgmistes keskkondades:
    - Windows 95 OSR2
    - Windows 98
    - Windows ME
    - Windows 2000 Professional Edition
    - Windows NT 4.0 SP6
    - Windows XP SP1
    - Windows XP SP2
- Moodul on testitud järgmistes veebilehitsejates:
    - Internet Explorer 5.01
    - Internet Explorer 5.5
    - Internet Explorer 6.0 SP1
    - Internet Explorer 6.0 SP2

Kasutusnäide

Fail: Test.vbs (visual basic script)

```
Option Explicit
Dim ISign

Set ISign= CreateObject("EIDCard.Sign")

wscript.echo "getInfo(): " & ISign.getInfo

wscript.echo "Allkirjastav sert: " & ISign.getSigningCertificate

wscript.echo
ISign.getSignedHash("0102030405060708090000A0B0C0D0e0F01020304",ISign.SelectedCe
rtNumber)
```

Allkirjastamine DigiDoc-iga

Kuna DigiDoc failide puhul kuulub allkirjastavate atribuutide hulka ka allkirjastaja sertifikaat (allkirja räsi on otseses sõltuvuses allkirjastaja sertifikaadist), siis on allkirjastamise käigus vajalik kiipkaardi poole pööruda kahel korral: esmalt sertifikaadi lugemiseks ja teistkordselt signeerimistoimingu teostamiseks.

signeerimine_samm1.html – näide veebilehel sertifikaadi lugemise kohta. Tüüpiline kasutusnäide allkirja ettevalmistamise sammul. Antud sammu käigus on mõistlik kasutajalt küsida ka muid allkirja atribuute: allkirjastamise asukohta ja rolli/resolutsiooni.

signeerimine_samm2.html – signeerimise näide. Eelnevalt on välja arvutatud allkirjastatav räsi ja on allkirjastamiseks kasutatava sertifikaadi järjenumber (mis loeti välja koos sertifikaadiga).