



**PRVÁ SLOVENSKÁ CERTIFIKAČNÁ AUTORITA  
(PSCA)**

# **iKey2000 - Inštaláčné inštrukcie**

Verzia dokumentu: **1.0**

Dátum vydania: **22.11.2005**

## Obsah

Obsah.....	2
1. �vod.....	3
2. Pojmy a skratky.....	4
3. Inštal�cia iKey 2000 softv�ru.....	5
3.1. Podmienky inštal�cie.....	5
3.2. Postup inštal�cie .....	5
4. Overenie funk�nosti iKEY2000 Series Software.....	12
5. Vyu�itie n�stroja spr�vy tokenov – CIP Utilities.....	13
5.1. Spustenie n�stroja CIP Utilities .....	13
5.2. Popis niektor�ch funkci� menu CIP Utilities Options .....	13
5.2.1. Prihl�senie sa do tokenu (Login).....	14
5.2.2. Zmena hesla (Passphrase) .....	15
5.2.3. Zmena menovky tokenu (personaliz�cia).....	16
5.2.4. Inicializ�cia tokenu .....	17
6. Prezeranie certifik�tov .....	19

# 1.  vod

 o je iKey?



iKey je finan ne nen ro n  autoriza n  predmet (token), pou iteln  na akomkoľvek PC, vybavenom USB portom.

iKey sp ja spoľahlivosť, jednoduchosť a bezpe nosť Smart-kariet a kryptografick ch tokenov, bez potreby pou itia  itacieho zariadenie a finan n ch n kladov na jeho zabezpe enie. iKey obsahuje pam ť na ulo enie osobn ch  dajov, certifik tov a hesiel. M  e byť pou it  na zabezpe enie e-mailov ch správ a ako autoriza n  predmet.

Produkt **iKey 2000 Series Authentication solution** je ur en  pre u ivateľov, ktorí pou ivaj  aplik cie vyu ivaj ce mo nosti certifik tov (napr. Entrust, Microsoft Outlook).

**iKey 2000 Series Software development Kit** je ur en  pre v voj arov softv ru, ktorí maj  z ujem implementovať iKey do vlastn ch produktov.

Nasleduj ce kroky opisuj  z kladn  in tal ciu a stru n  vysvetlenie funkcionality produktu *iKey 2000 Series*.

## 2. Pojmy a skratky

**Token** – autorizačný predmet (SmartCard, USB kľúč)

**Prihlásenie sa** – Zadanie identifikačných údajov (meno a heslo u ivateľa) pri zapnutí operačného systému

**Voľba, zvolenie** – označenie komponentu kurzorom myši, n sledn  kliknutie ľavým tlačidlom (Voľba bude označen /zvolen )

**USB** – štandardn  zbernica osobn ho po itača podporuj ca prenosov  r chlosti a  12 MB/s a umo n uj ca pripojiť a  127 druhov r znych zariaden  (myš, modem, kl vesnica, token ap.)

**PC** – osobn  po itač (Personal Computer)

**CD** – diskov  z znamov  m di m (Compact Disc)

**DVD** – optick  z znamov  m di m (Digital Versatile Disc)

**PSCA** – Prv  Slovensk  Certifikačná Autorita

## 3. Inštalácia iKey 2000 softvéru

### 3.1. Podmienky inštalácie

Musí byť nainštalovaný operačný systém Windows vo verziách:

- Windows 95 OSR 2.5 a vyšší
- Windows 98 SE
- Windows NT 4.0 SP 6a a vyšší
- Windows 2000 SP 2 a vyšší
- Windows XP Professional

Pre úspešnú inštaláciu na systémy Windows XP, 2000, alebo NT 4.0 je nutné prihlásiť sa do systému ako užívateľ s **oprávnením administrátora**.

Token nesmie byť počas inštalácie pripojený k počítaču

**Poznámka:** V prípade, že token je pripojený v USB porte, je ho potrebné odpojiť!

### 3.2. Postup inštalácie

1. Zavrieť všetky otvorené programy a aplikácie, odpojiť tokeny zo systému.
2. Odinštalovať všetky predchádzajúce verzie softvéru iKey 2000, ak boli nainštalované.
3. Do CD/DVD mechaniky vložiť inštalčné CD programu iKey 2000. Inštalčný program sa spustí automaticky (ak je povolená funkcia Autorun). V opačnom prípade vyhľadať a spustiť program **start.exe** z inštalčného CD.

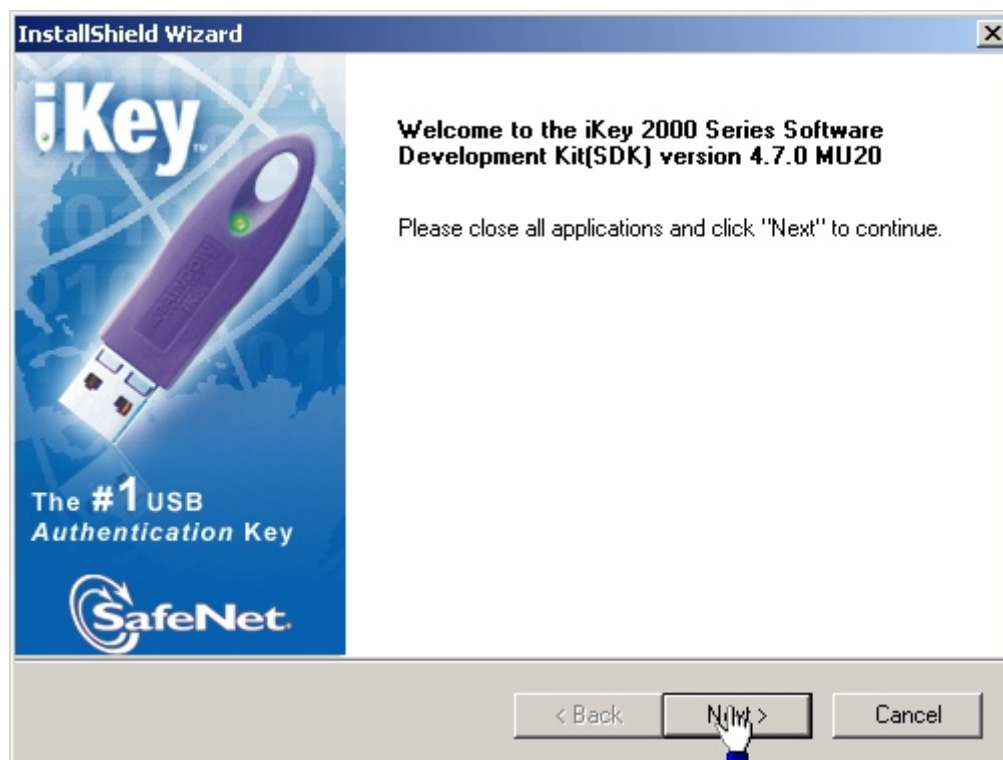
4. V úvodnom okne kliknúť na **“Install SafeNet iKey 2000 Series Software development Kit v4.7.0 with MU20“**.



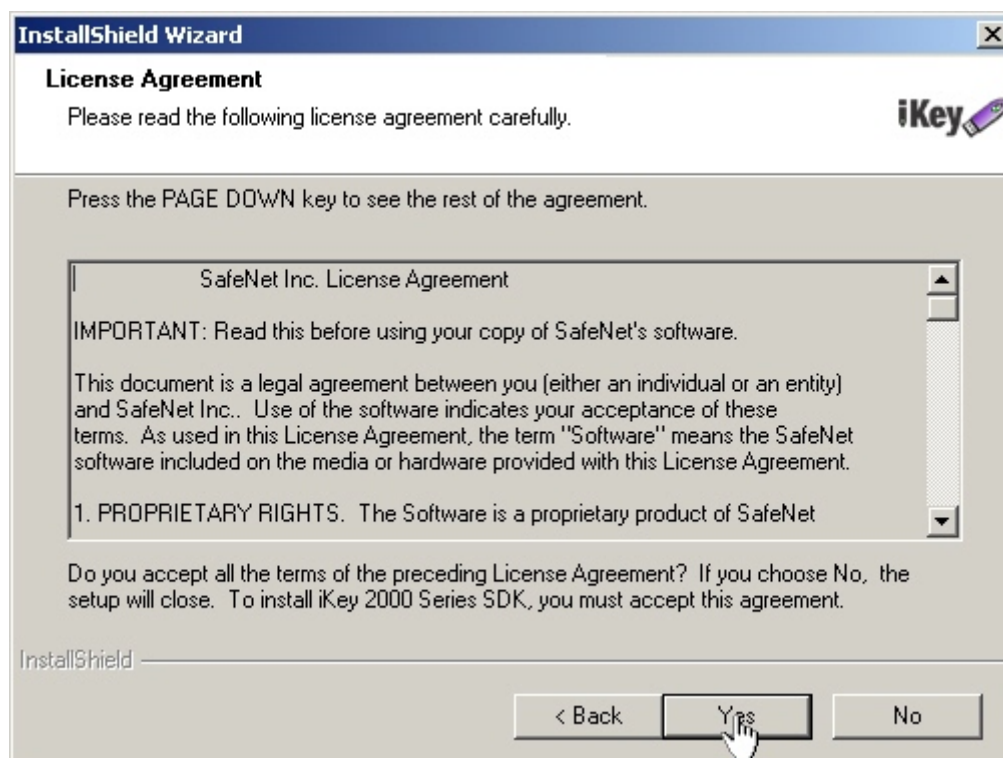
5. Po príprave inštalácie sa automaticky zobrazí uvítacie okno.



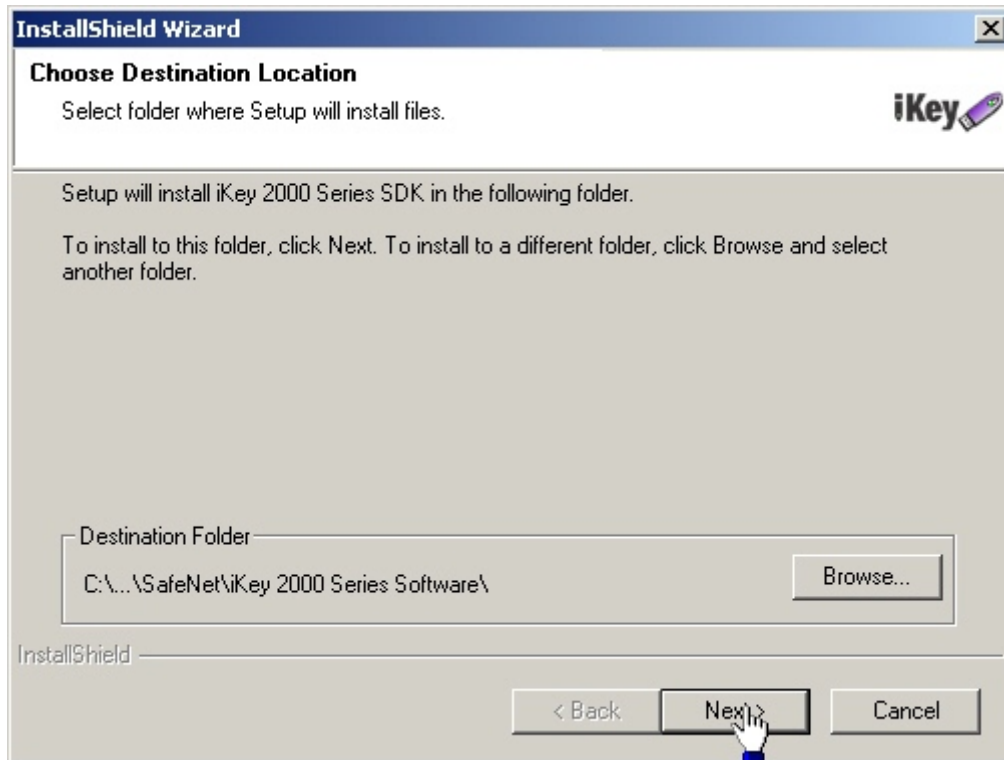
6. V uvítacom okne **InstallShield Wizard** pokračovať kliknutím na **NEXT**.



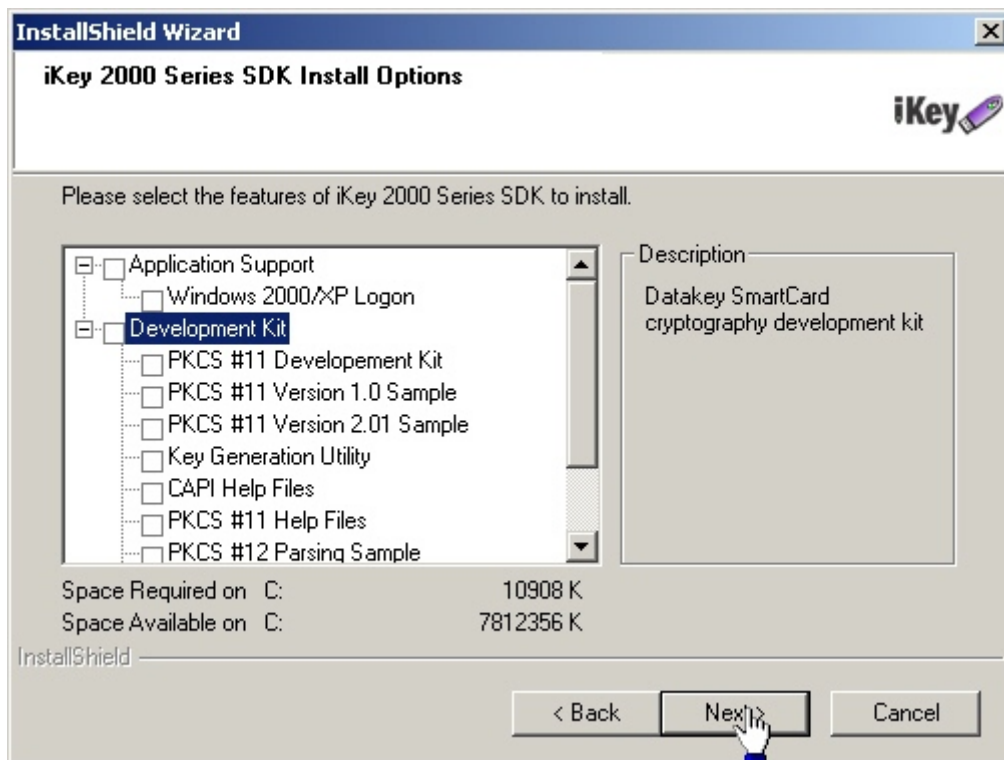
7. Súhlas s licenčnými podmienkami potvrdiť kliknutím na **YES**.



8. Zvoliť adresár, kde bude aplikácia nainštalovaná a pokračovať kliknutím na **NEXT**. V prípade, že nechcete použiť prednastavený adresár použiť tlačidlo **BROWSE** a zvoliť iný adresár na inštaláciu.

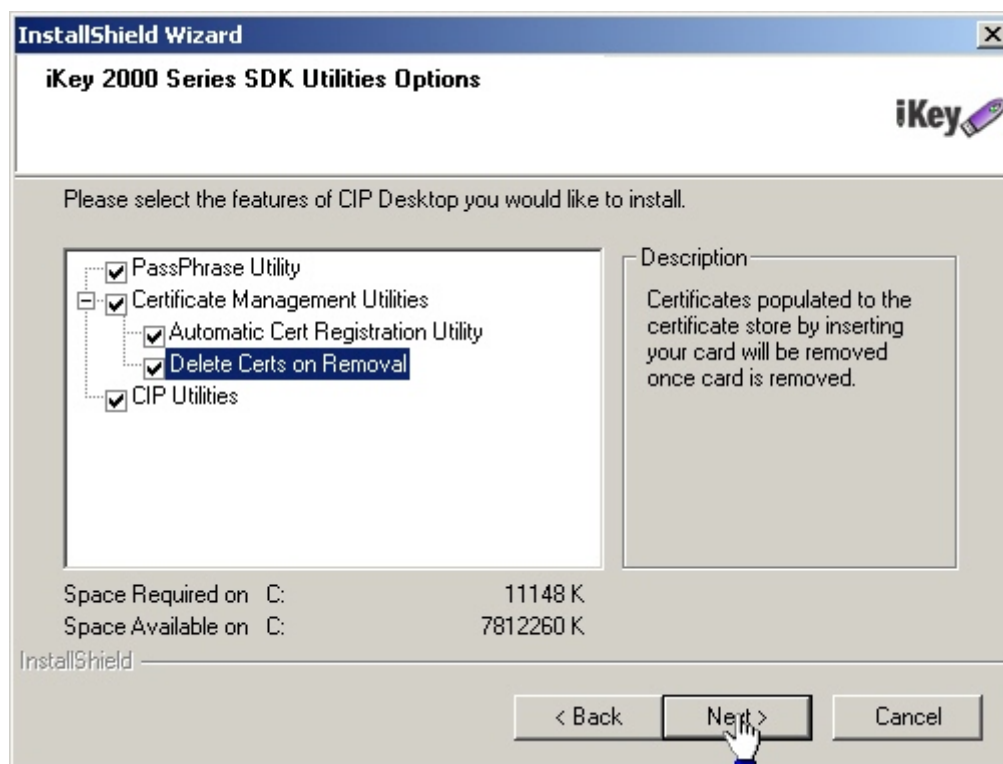


9. V okne **iKey 2000 Series SDK Install Options** zrušiť voľbu všetkých zobrazených komponentov, ktoré sú štandardne predvolené na inštaláciu a pokračovať kliknutím na **NEXT** (pozri obrázok).



**Poznámka:** V prípade, že potrebujete použiť Váš iKey token pri prihlasovaní sa do systému Windows (iKey token musí obsahovať certifikát na prihlasovanie sa do Windows) vyberte možnosť Windows 2000/XP logon

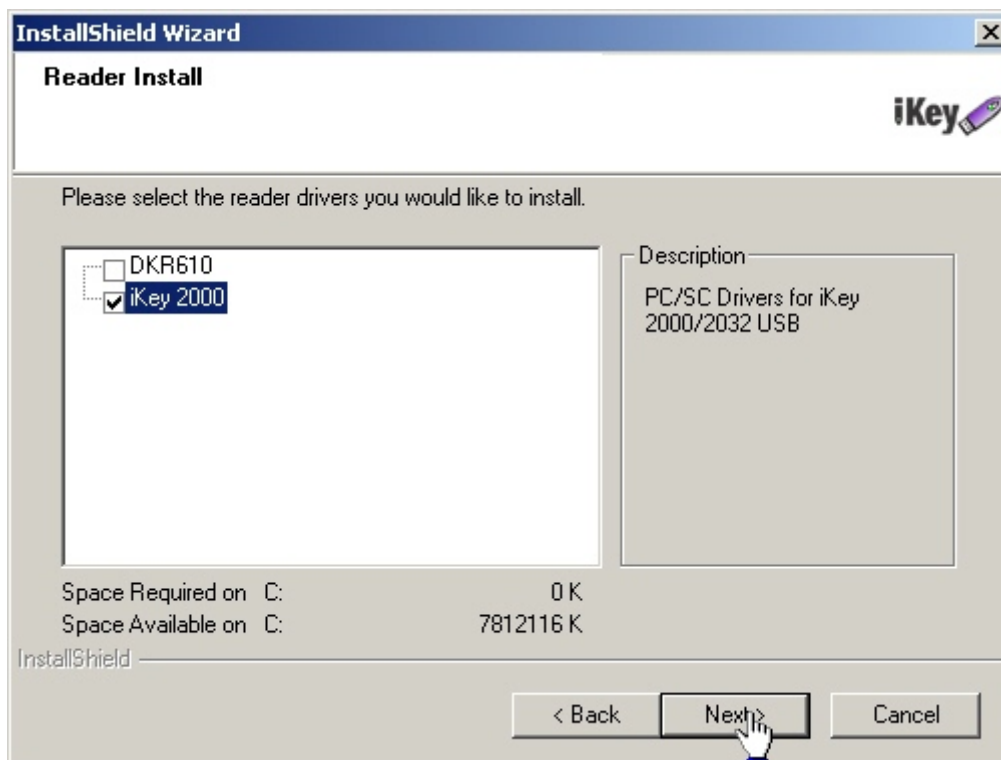
10. V okne **iKey 2000 Series SDK Utilities Options** vyberte všetky ponúkané možnosti (pozri obrázok) a pokračujte voľbou **NEXT**.



Význam jednotlivých volieb:

- |                                     |   |   |
|-------------------------------------|---|---|
| PassPhrase Utility                  | – | Nástroj na zmenu prednastaveného hesla  |
| Automatic Cert Registration Utility | – | Automatické načítanie certifikátov po vložení tokenu  |
| Delete Certs on Removal             | – | Načítané certifikáty sa vymažú z operačného systému pri odstránení tokenu z USB portu (zvýšená ochrana proti zneužitiu) |
| CIP Utilities                       | – | Nástroj pre správu SmartCard  |

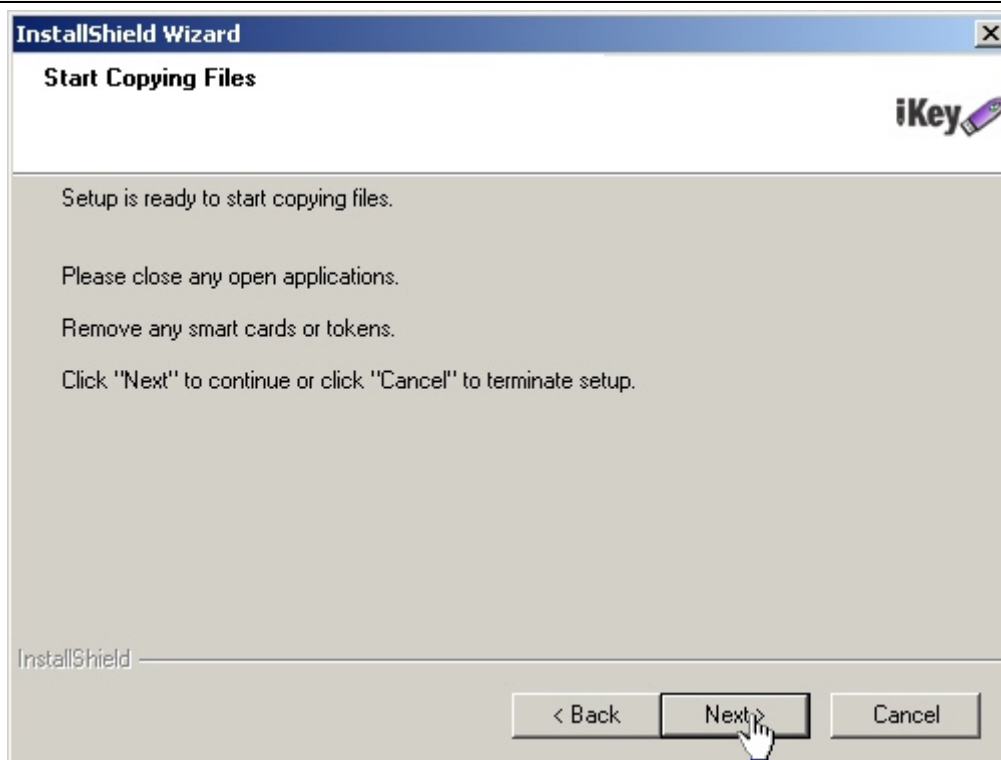
11. V okne **Reader Install** vybrať ovládače pre použitý autorizačný token (iKey 2000) a pokračovať kliknutím **NEXT**.



**Upozornenie:** V prípade, že máte nainštalovaný Netscape Navigator, zobrazí sa okno potvrdenia inštalácie bezpečnostného modulu pre tento program. Na pokračovanie zvolíť **OK**.

12. V okne **Start Copying Files** pokračovať v inštalácii kliknutím na **NEXT**

**Upozornenie:** V USB porte **nesmie** byť vložený iKey token! Odporúča sa **ukončiť** všetky bežiace aplikácie!.



13. V okne **InstallShield Wizard Complete** si inštalácia vyžiada reštart systému. Zvoliť **“Yes, I want to restart my computer now.”**. Pokračovať kliknutím na **Finish**.



14. Po reštarte a prihlásení sa do systému bude inštalácia softvéru iKey automaticky dokončená.

## 4. Overenie funkčnosti iKEY2000 Series Software

Overenie funkčnosti nainštalovaného softvéru iKey sa vykoná nasledovným spôsobom:

1. Vložiť token do niektorého USB portu na vašom počítači
2. Spustiť aplikáciu CIP Utilities kliknutím na **ŠTART** (START v anglickej verzii Windows), následne na **Programy (Programs) → SafeNet → iKey 2000 Series Software → CIP Utilities**



3. Po spustení programu, v prípade, že USB token obsahuje aspoň jeden certifikát, by ste mali vidieť podobný výstup ako je znázornený na obrázku. Za označeniami **Certificate** a **Key** je v zátvorke uvedené CKA\_LABEL daného páru kľúčov a certifikátu – z obrázku bolo toto označenie odstránené):



## 5. Využitie nástroja správy tokenov – CIP Utilities.

Programový nástroj CIP Utilities obsahuje niekoľko nástrojov na správu tokenov iKey. V nasledovnom si popíšeme len nástroje, ktoré sú potrebné pre bežnú prácu s tokenom.

### 5.1. Spustenie nástroja CIP Utilities

Spustiť aplikáciu CIP Utilities kliknutím na **ŠTART** (START v anglickej verzii Windows), následne na **Programy (Programs) → SafeNet → iKey 2000 Series Software → CIP Utilities**



### 5.2. Popis niektorých funkcií menu CIP Utilities Options

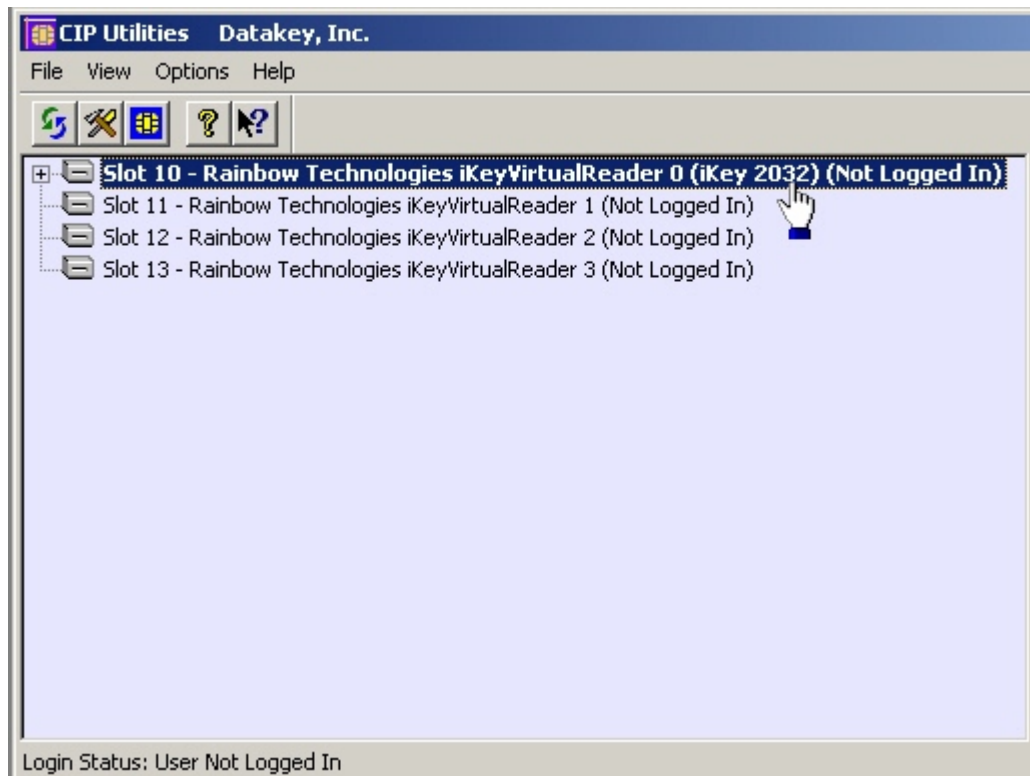
Funkcie menu programu CIP Utilities (pozri obrázok), ktoré sú povolené pomocou **Options → Configuration** je možné pre jednotlivé sloty, v ktorých sa príslušný token nachádza, vybrať a spustiť kliknutím pravým tlačidlom myši na daný slot.



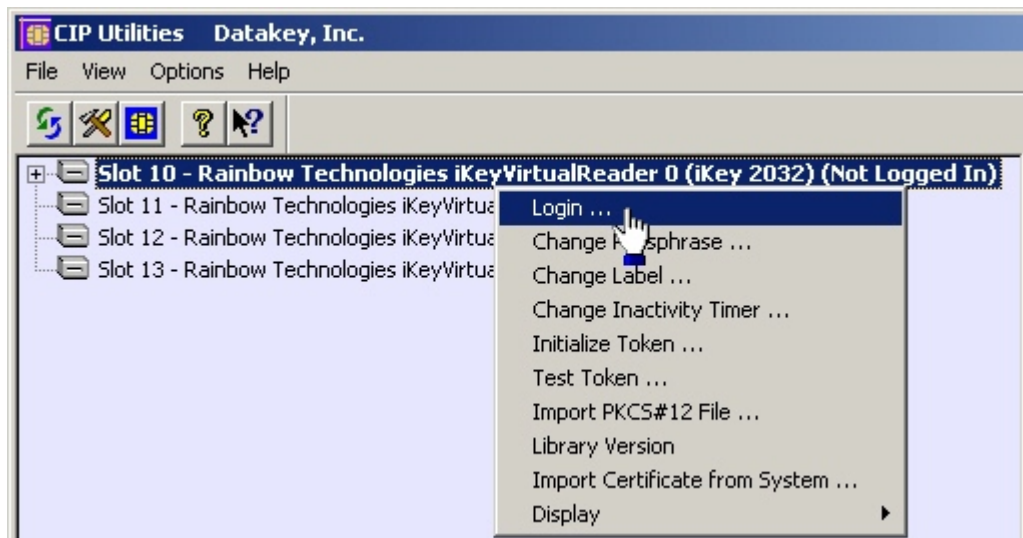
V nasledujúcich odsekoch je uvedený popis najpoužívanejších položiek z hľadiska bežného používateľa CIP Utilities hore uvedeného menu.

### 5.2.1. Prihlásenie sa do tokenu (Login)

Do tokenu sa je možné prihlásiť kliknutím pravého tlačidla myši na príslušný slot, v ktorom sa token nachádza (označený **iKey 2032**(Not Logged In))



a následným zvolením prvej položky v ponukovom menu s názvom **Login....**

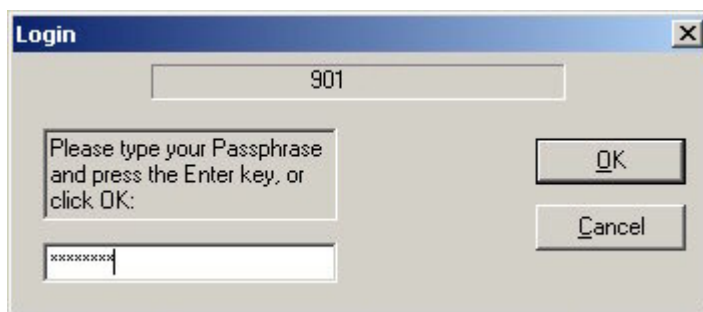


Pri prihlásení sa k tokenu (**Login**) je vyžadované heslo (**Passphrase**). Zadáva sa do prázdnej kolónky vľavo dole. Zadať heslo (pozri Upozornenie) a pokračovať kliknutím na **OK**.

---

**Upozornenie:** V prípade, že token používate prvý krát (štandardné heslo nebolo menené) použite heslo: **PASSWORD**, ktoré je platné pre všetky nové tokeny.

---



Po prihlásení sa k tokenu zodpovedajúcim heslom je možné vykonávať ďalšie operácie s tokenom.

### 5.2.2. Zmena hesla (Passphrase)

Zmenu hesla je vhodné vykonať čo najskôr po uložení prvých kľúčov na token, aby sa predišlo prípadnému zneužitiu tokenu. Prednastavené heslo (PASSWORD) je možné zmeniť nasledovným postupom:

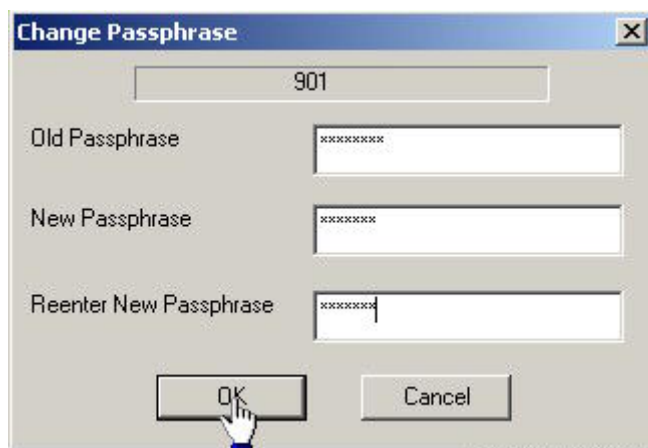
1. Kliknúť pravým tlačidlom myši na príslušný slot, v ktorom sa token nachádza.
2. Vybrať položku **Change Passphrase** z menu (pozri obrázok).

**Upozornenie:** V prípade, že nebolo pred zmenou hesla vykonané prihlásenie sa do tokenu [stav tokenu v slotě (iKey 2032)(Not Logged In)] budete pred zmenou hesla požadovaný o prístupové heslo.



3. V okne **Change Passphrase** zadať do voľných riadkov informácie v poradí:
  - Staré heslo (Old Passphrase)
  - Nové heslo (New Passphrase)
  - Opakovane nové heslo na jeho potvrdenie (Reenter New Passphrase)

**Poznámka:** Minimálna dĺžka hesla je 4 znaky a maximálna dĺžka je 20 znakov

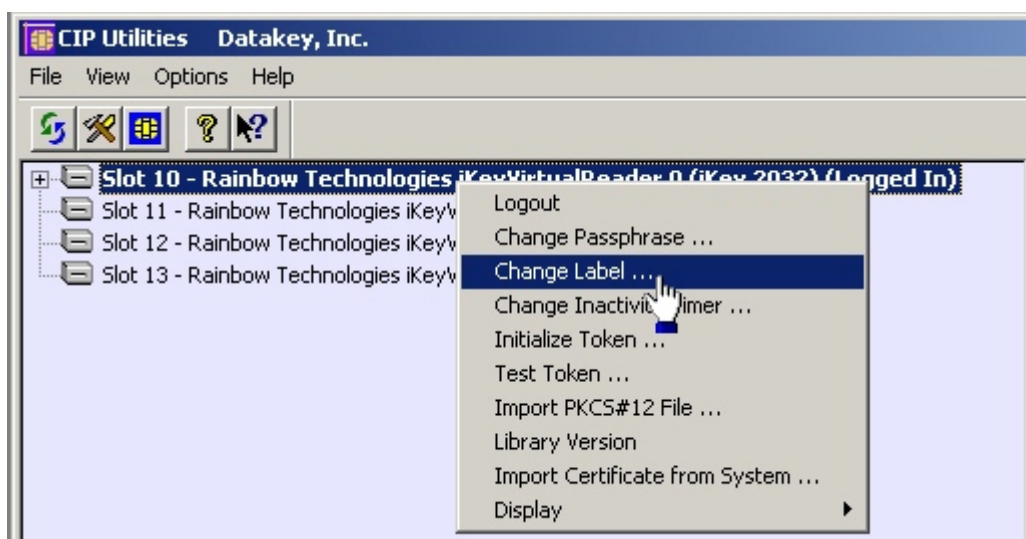


15. Potvrdiť zmenu hesla kliknutím na **OK**.

### 5.2.3. Zmena menovky tokenu (personalizácia)

Menovka tokenu (Label) je použité pre lepšiu orientáciu v prípade využívania viacerých tokenov a jednoduchú identifikáciu konkrétneho tokenu. Menovku je možné zmeniť nasledovným spôsobom (prednastavená menovka je sériové číslo tokenu):

1. Kliknúť pravým tlačidlom myši na príslušný slot, v ktorom je vložený iKey token
2. Zvoliť z menu položku **Change label** (pozri obrázok).



3. Zmeniť pôvodnú menovku nastavenú výrobcom (sériové číslo tokenu) na novú menovku – napr. meno majiteľa ap.



4. Po ukončení zadávania odsúhlasiť zmenu menovky kliknutím na OK.

#### 5.2.4. Inicializácia tokenu

Inicializácia tokenu slúži na jeho nastavenie do pôvodného stavu t.j. stavu pred umiestnením akýchkoľvek kľúčov, certifikátov a iných informácií. Inicializácia odstráni z kľúča všetky existujúce položky (kľúče, certifikáty atď.) a ponechá nedotknuté len sériové číslo tokenu a jeho menovku.

#### **DÔLEŽITÉ UPOZORNENIE !!!**

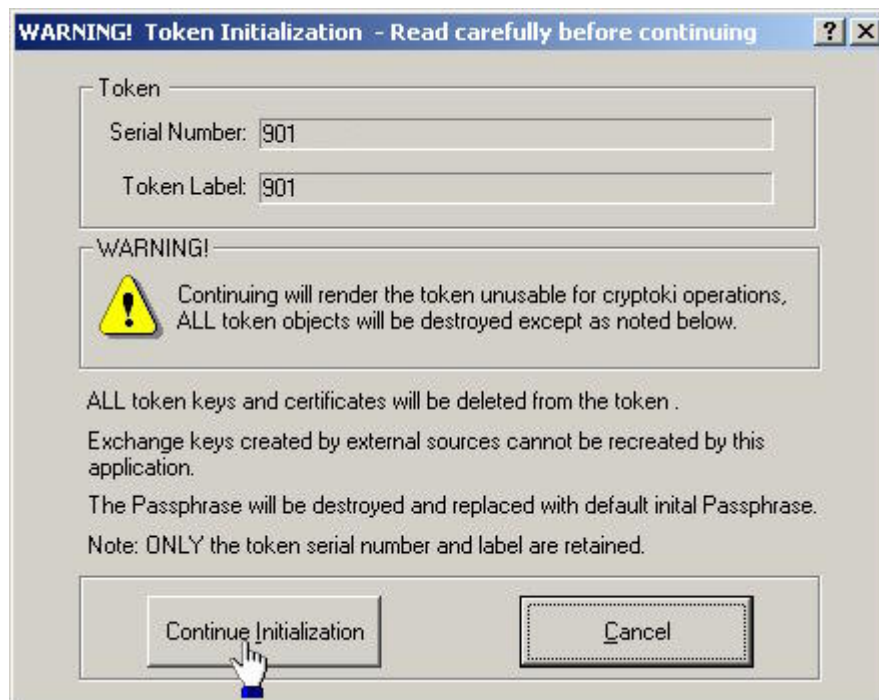
**Tento postup použiť len v prípade, že došlo k zablokovaniu tokenu a nie je možné ďalej používať kľúče a certifikáty na ňom uložené. Pri inicializácii budú všetky údaje z tokenu nenávratne odstránené!!!**

Inicializácia sa vykoná podľa nasledovného postupu:

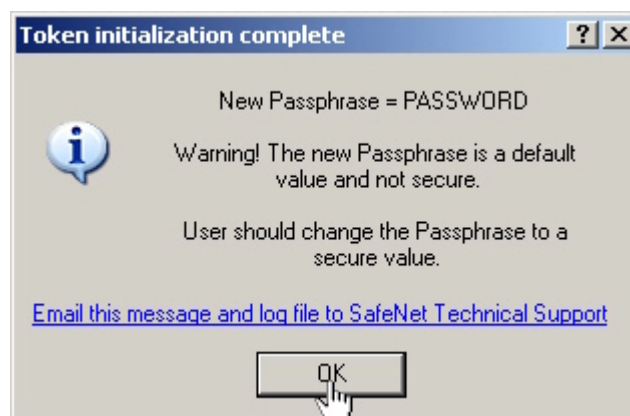
1. Kliknúť pravým tlačidlom myši na príslušný slot, a príslušný slot, v ktorom sa token nachádza
2. Zvoliť z kontextového menu položku **Initialize Token** (pozri obrázok)



- Po zobrazení varovného hlásenia o vymazaní všetkých údajov a zmene hesla na prednastavené heslo pokračovať kliknutím na **Continue Initialization**.



- Po zobrazení upozornenia na úspešné ukončenie inicializácie a zmenu hesla na prednastavené (*PASSWORD*) pokračovať kliknutím na **OK**.

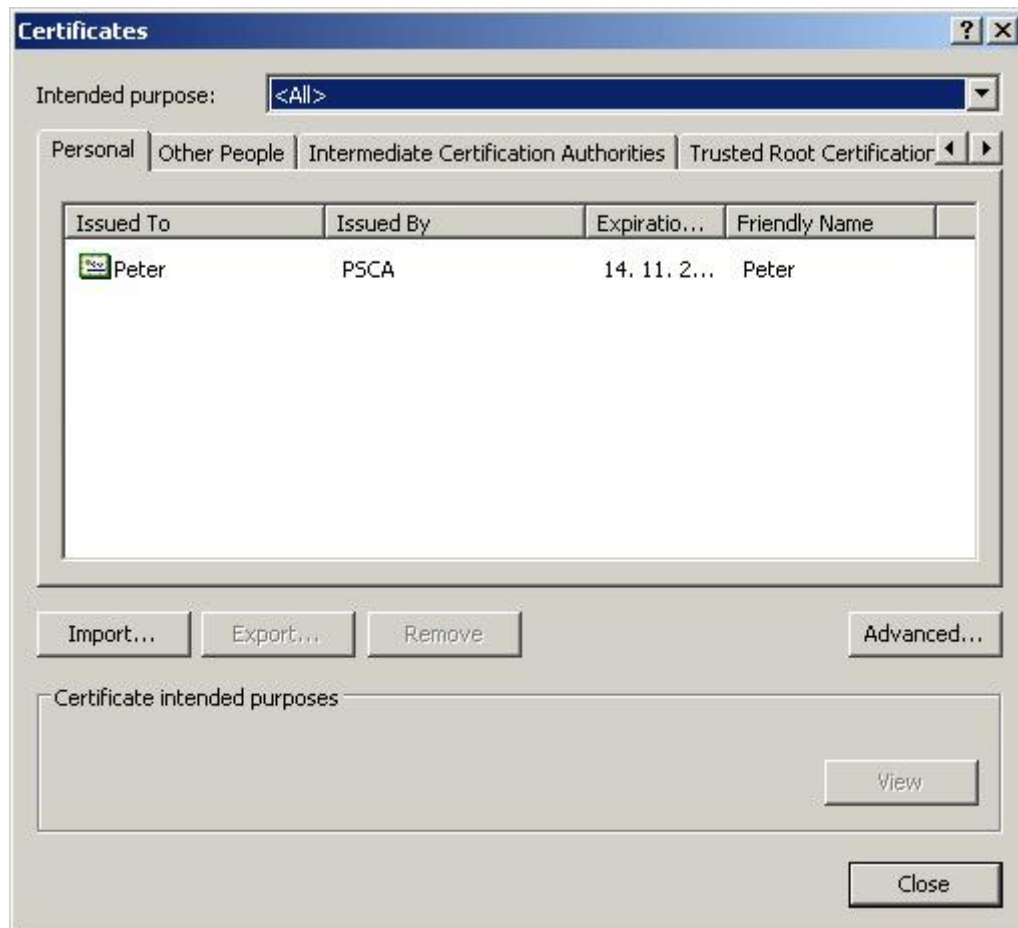


Týmto je inicializácia tokenu ukončená a všetky pôvodné údaje s výnimkou sériového čísla (Serial Number) a menovky (Label) z neho boli odstránené.

## 6. Prezeranie certifikátov

Ak chcete vidieť certifikáty (token musí byť vložený v USB porte), ktoré máte k dispozícii, je potrebné vybrať vo vašom prehliadači (Internet Explorer) nasledovné príkazy menu (anglická verzia a slovenská verzia)

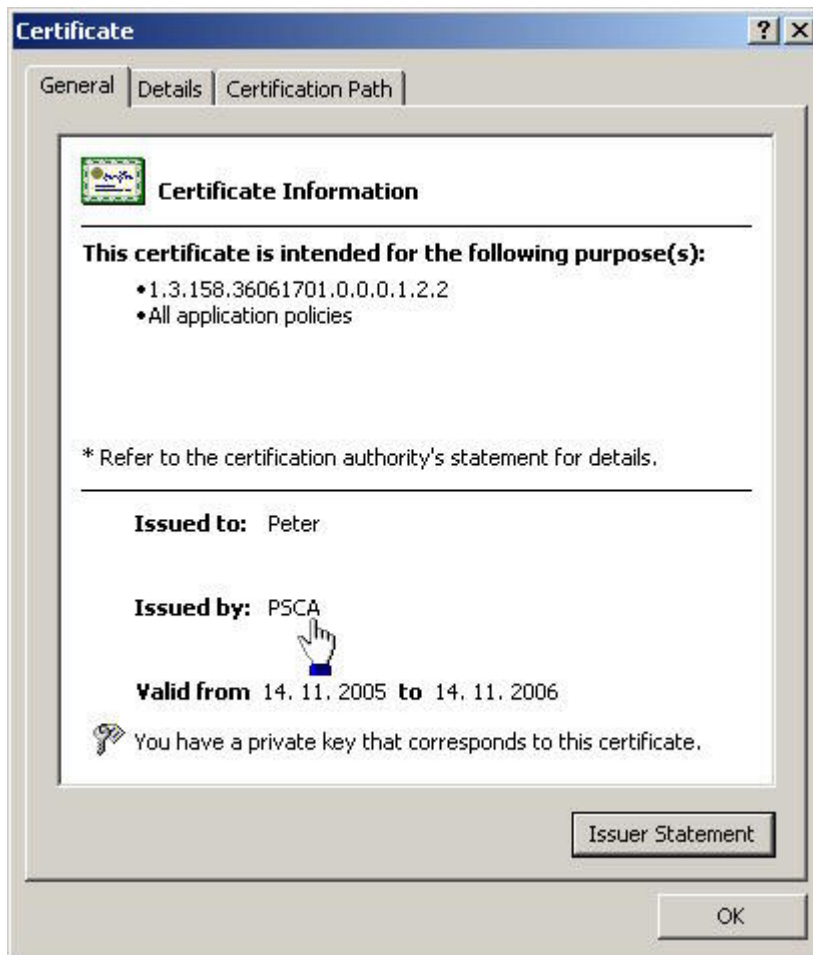
**Tools → Internet Options... → Content → Certificates...**  
**Nástroje → Možnosti siete Internet... → Obsah → Certifikáty...**



V okne **Certificates (Certifikáty)** sa zobrazí zoznam certifikátov, ktoré má váš systém k dispozícii.

Certifikát verejného kľúča kvalifikovaného certifikátu vydaného Prvou slovenskou certifikačnou autoritou (PSCA), prevádzkovanou spoločnosťou Viasec, s.r.o, je certifikát, ktorý má v stĺpci **Issued By (Vydavateľ)** uvedené „**PSCA**“ (pozri predchádzajúci obrázok).

Pre podrobnejšie informácie o certifikáte je potrebné dva krát kliknúť na daný certifikát pričom sa zobrazí nasledovná informácia:



V položke **Issued to: (Vydané pre:)** je uvedené meno držiteľa certifikátu, v položke **Issued by: (Vydavateľ:)** je uvedené označenie certifikačnej autority, ktorá certifikát vydala a v položke **Valid from .. to .. (Platný od .. do ..)** je uvedená doba platnosti daného certifikátu.

Podrobnejšie informácie o certifikáte môžete nájsť v záložke **Details (Podrobnosti)**.

Podrobné informácie o vydavateľovi sú uvedené v položke **Issuer (Vydavateľ)** a podrobné informácie o držiteľovi v položke **Subject (Subjekt)**, tak ako to môžete vidieť na dole uvedených obrázkoch. V ostatných položkách sú uvedené ďalšie informácie požadované pre daný druh certifikátu.

