GINIT

Užívateľský manuál

Máj 2011

SOFTIDEA

Obsah

Zoznam obrázkov

1 Úvod

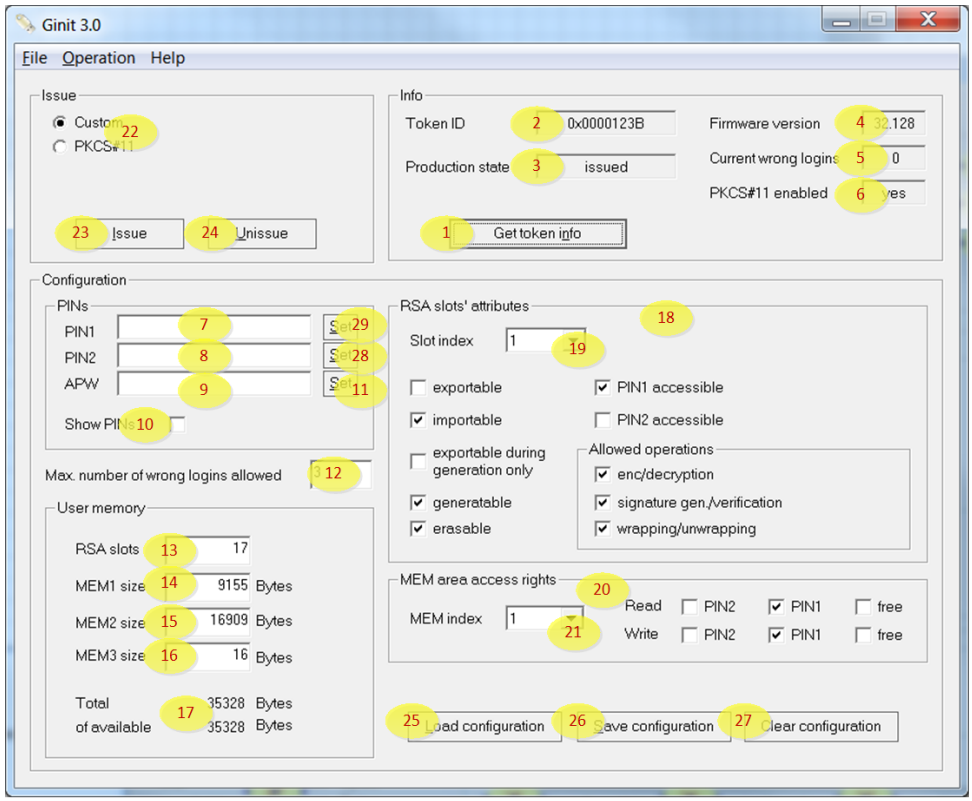
Aplikácia GINIT je určená pre administráciu kryptografických zariadení GNT USB Token [1] bezpečnostným správcom ("*Administrátor*"). Umožňuje zobraziť informácie a nastavenia Tokenu, meniť heslo administrátora Tokenu (*APW*) a heslá užívateľa *PIN1* a *PIN2*. Ďalej umožňuje realizovať nasledujúce prechody medzi jednotlivými stavmi životného cyklu Tokenu:

- inicializovať Token pre použitie koncovým užívateľom, to znamená definovať bezpečnostnú politiku používania Tokenu,
- deinicializovať Token, to znamená zmazať všetky užívateľské nastavenia a uviesť Token do počiatočného výrobného stavu.

Aplikácia GINIT umožňuje pracovať v danom čase s jedným Tokenom prítomným v systéme. Ak sú prítomné viaceré Tokeny, alebo nieje prítomný žiadny Token, aplikácia na to upozorní chybovou správou.

2 Užívateľské rozhranie

Hlavným zobrazením užívateľského rozhrania aplikácie GINIT je dialógové okno znázornené na obrázku 1. Význam jednotlivých prvkov tohoto dialógového okna je popísaný v nasledujúcom texte.



Obrázok 1: Hlavné zobrazenie užívateľského rozhrania GINIT

1. Tlačidlo *Get token info*: Prečíta a zobrazí informácie o Tokene.
2. Pole *Token ID*: Zobrazuje jedinečný identifikátor Tokenu.
3. Pole *Production state*: Zobrazuje aktuálny stav životného cyklu Tokenu.
4. Pole *Firmware version*: Zobrazuje verziu firmvéru Tokenu.
5. Pole *Curent wrong logins*: Zobrazuje aktuálny stav počítadla neúspešných loginov.
6. Pole *PKCS#11 enabled*: Signalizuje, či je token inicializovaný pre rozhranie SIPKCS [2].
7. Pole *PIN1*: Umožňuje nastaviť prístupové heslo užívateľa PIN1.
8. Pole *PIN2*: Umožňuje nastaviť prístupové heslo užívateľa PIN2.
9. Pole *APW*: Umožňuje nastaviť prístupové heslo administrátora APW.
10. Volič *Show PINs*: Umožňuje povoliť, alebo zakázať zobrazenie hesiel.
11. Tlačidlo *Set*: Nastaví, alebo zmení heslo *APW* na hodnotu nastavenú v poli *APW*.
12. Pole *Max number of wrong logins allowed*: Umožňuje definovať maximálny počet neúspešných loginov. Po prekročení tejto hodnoty sa token vráti do výrobného stavu.
13. Pole *RSA Slots*: Počas inicializácie umožňuje definovať počet RSA buniek. V prípade vydaného Tokenu zobrazuje nastavený počet RSA buniek.
14. Pole *MEM1 size*: Počas inicializácie umožňuje nastaviť veľkosť oblasti MEM1. V prípade vydaného Tokenu zobrazuje nastavenú veľkosť oblasti MEM1.
15. Pole *MEM2 size*: Počas inicializácie umožňuje nastaviť veľkosť oblasti MEM2. V prípade vydaného Tokenu zobrazuje nastavenú veľkosť oblasti MEM2.
16. Pole *MEM2 size*: Počas inicializácie umožňuje nastaviť veľkosť oblasti MEM3. V prípade vydaného Tokenu zobrazuje nastavenú veľkosť oblasti MEM3.
17. Pole *Total X of available Y*: Zobrazuje celkovú veľkosť (*Y*) užívateľskej pamäti Tokenu a veľkosť pamäti (*X*) použitej pre nastavenú konfiguráciu.
18. Skupina prvkov *RSA Slots attributes*: Počas inicializácie umožňuje definovať atribúty jednotlivých RSA buniek. V prípade vydaného Tokenu zobrazuje nastavené atribúty jednotlivých RSA buniek.
19. Pole *Slot index*: Definuje poradové číslo RSA bunky, ktorej atribúty sú zobrazené v skupine prvkov (18). Maximálna hodnota tohoto poľa je rovná hodnote poľa (13).
20. Skupina prvkov *MEM area acess rights*: Počas inicializácie umožňuje definovať prístupové práva k jednotlivým MEM oblastiam. V prípade vydaného Tokenu

zobrazuje nastavené prístupové práva k jednotlivým MEM oblastiam.

21. Pole *MEM index*: Definuje poradové číslo MEM oblasti, ku ktorej prístupové práva sú zobrazené v skupine prvkov (20).

22. Prepínač *Issue*: Pri inicializácii Tokenu umožňuje prepínať medzi užívateľským nastavením (*Custom*) a nastavením pre rozhranie SIPKCS (*PKCS #11*).

23. Tlačidlo *Issue*: Vykoná inicializáciu Tokenu podľa nastavených parametrov.

24. Tlačidlo *Unissue*: Vykoná deinicializáciu Tokenu.

25. Tlačidlo *Load configuration*: Umožní načítať existujúcu konfiguráciu zo súboru.

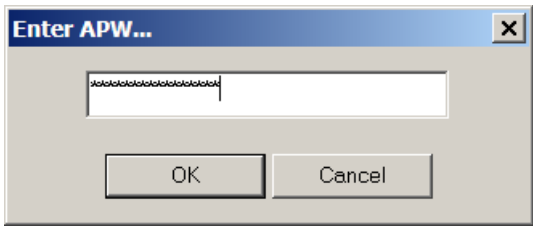
26. Tlačidlo *Save configuration*: Umožní uložiť nastavenú konfiguráciu do súboru.

27. Tlačidlo *Clear configuration*: Umožní vymazať nastavenia konfigurácie.

28. Tlačidlo *Set*: Nastaví, alebo zmení heslo *PIN2* na hodnotu nastavenú v poli *PIN2*.

29. Tlačidlo *Set*: Nastaví, alebo zmení heslo PIN1 na hodnotu nastavenú v poli *PIN1*.

Niektoré operácie vyžadujú autentifikáciu administrátora heslom *APW,* prípadne heslom *PIN2*. Vtedy GINIT vyzve na zadanie príslušného hesla dialógom znázorneným na obrázku 2.



Obrázok 2: Výzva na vloženie hesla

3 Operácie

3.1 Načítanie aktuálnej konfigurácie Tokenu

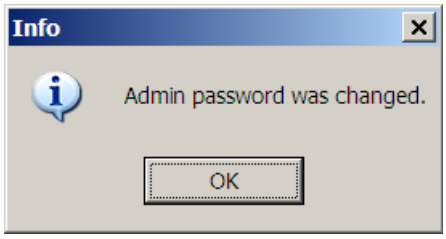
Načítanie aktuálnej konfigurácie Tokenu sa vykoná stlačením tlačidla "*Get token info*" (prvok 1. na obrázku 1). Aplikácia GINIT nadviaže spojenie s Tokenom prítomným v systéme a vyžiada si jeho aktuálnu konfiguráciu. Po úspešnom vykonaní tejto operácie jednotlivé prvky užívateľského rozhrania (okrem polí znázorňujúcich prístupové heslá) zobrazujú hodnoty aktuálnej konfigurácie Tokenu. Rozsah zobrazených údajov závisí od aktuálneho stavu životného cyklu Tokenu.

3.2 Zmena prístupového hesla *APW*

Zmenu *APW* vykoná administrátor nasledujúcim spôsobom:

- nastaví novú hodnotu *APW* v poli *APW* (prvok 8. na obrázku 1),
- stlačí tlačidlo *Set* (prvok 11. na obrázku 1),
- po vyzvaní zadá staré heslo *APW*.

Úspešné dokončenie operácie je signalizované dialógom znázorneným na obrázku 3.



Obrázok 3: Potvrdenie o úspešnej zmene hesla

Poznámka: Zmenu hesla *APW* je tiež možné vykonať ako súčasť inicializácie Tokenu (kapitola3.5) tak, že pred vydaním Tokenu tlačidlom *Issue* sa vyplní nové heslo *APW* do poľa *APW*.

3.3 Zmena prístupového hesla *PIN2*

Zmenu *PIN2* inicializovaného Tokenu je možné vykonať v aplikácii GINIT nasledujúcim spôsobom:

- nastaviť novú hodnotu *PIN2* v poli *PIN2* (prvok 8. na obrázku 1),
- stlačiť tlačidlo *Set* (prvok 28. na obrázku 1),
- po vyzvaní zadať staré heslo *PIN2*.

Úspešné dokončenie operácie je signalizované potvrdzujúcim dialógom.

Poznámka: Bez znalosti pôvodného hesla PIN2 nieje možné aplikovať vyššie uvedený postup. V takom prípade je možné zmeniť heslo PIN2 len deinicializáciou a následnou novou inicializáciou Tokenu (kapitoly 3.5 a 3.6).

3.4 Zmena prístupového hesla *PIN1*

Zmenu *PIN1* inicializovaného Tokenu, napríklad po jeho strate užívateľom, je možné vykonať v aplikácii GINIT nasledujúcim spôsobom:

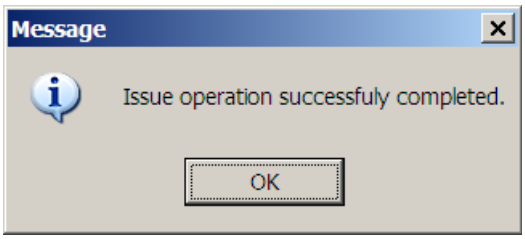
- nastaviť novú hodnotu *PIN1* v poli *PIN1* (prvok 7. na obrázku 1),
- stlačiť tlačidlo *Set* (prvok 29. na obrázku 1),
- po vyzvaní zadať heslo *PIN2*.

Úspešné dokončenie operácie je signalizované potvrdzujúcim dialógom.

Poznámka: Bez znalosti hesla PIN2, alebo pôvodného hesla PIN1 nieje možné zmeniť PIN1. V takom prípade je možné zmeniť heslo PIN1 len deinicializáciou a následnou novou inicializáciou Tokenu (kapitoly 3.5 a 3.6).

3.5 Inicializácia Tokenu

Inicializáciou Tokenu (ďalej tiež "vydanie Tokenu") rozumieme nastavenie užívateľskej konfigurácie Tokenu v súlade s bezpečnostnou politikou, nastavenie počiatočných prístupových hesiel užívateľa a vydanie Tokenu do používania užívateľovi. Technicky sa jedná o vykonanie prechodu "*issue*" životného cyklu Tokenu, popísaného v katalógovom liste [1]. Vydanie Tokenu obvykle realizuje bezpečnostný správca organizácie, ktorý disponuje prístupovým heslom administrátora Tokenu *APW*. Počiatočné prístupové heslo administrátora Tokenu *APW* nastavené výrobcom je *"admin"*. Aby mohol byť Token vydaný, musí byť v stave "nevydaný - *unissued*". Ak prepínač *Issue* (prvok 23. na obrázku 1) je v polohe *Custom*, je možné nastaviť všetky prvky užívateľskej konfigurácie v plnom rozsahu povolených hodnôt. Nastavené hodnoty je možné pomocou tlačidiel 25-27 na obrázku 1 uložiť do súboru a nahrať zo súboru. Ak prepínač *Issue* (prvok 23. na obrázku 1) je v polohe *PKCS#11*, niektoré prvky užívateľského rozhrania nie sú prístupné. Viac informácií o inicializácii Tokenu pre rozhranie SIPKCS je v kapitole3.5.1. Po nastavení hodnôt užívateľskej konfigurácie administrátor stlačením tlačidla *Issue* zrealizuje vydanie Tokenu. Ak administrátor nebol doposiaľ autentifikovaný, je požiadaný o vloženie hesla *APW* dialógom na obrázku 2. Úspešné dokončenie inicializácie je signalizované dialógom znázorneným na obrázku 4.



Obrázok 4: Potvrdenie o úspešnom dokončení inicializácie Tokenu

3.5.1 Inicializácia Tokenu pre rozhranie SIPKCS

Rozhranie SIPKCS [2] je implementáciou štandardného rozhrania PKCS #11 [3] pre prístup k hardvérovým kryptografickým zariadeniam. Postup inicializácie nevydaného Tokenu pre rozhranie SIPKCS je nasledujúci:

- prepínač *Issue* prepnúť do polohy *PKCS#11*,
- nastaviť počiatočné heslo užívateľa *PIN1*,
- voliteľne nastaviť nové heslo administrátora *APW*,
- stlačiť tlačidlo *Issue*

- po vyzvaní zadať platné heslo *APW*.

Poznámka: Načítanie konfigurácie Tokenu už inicializovaného pre rozhranie SIPKCS a inicializácia iného Tokenu s takouto konfiguráciou nieje ekvivalentná inicializácii s prepínačom Issue nastaveným do polohy PKCS#11. Inicializácia pre SIPKCS vyžaduje navyše zápis konfiguračných údajov do oblasti MEM3, ktorý sa vykoná len ak prepínač Issue je v *polohe PKCS#11.*

Po načítaní aktuálnej konfigurácie (kapitola 3.1) Tokenu inicializovaného pre rozhranie SIPKCS je podpora rozhrania signalizovaná prítomnosťou hodnoty "*yes*" v poli "*PKCS#11 enabled*" (prvok 6. na obrázku 1). Podrobné informácie o rozhraní SIPKCS a o jeho použití sú dostupné v dokumente [2].

3.6 Deinicializácia Tokenu

Deinicializáciou Tokenu rozumieme výmaz užívateľskej konfigurácie Tokenu a nastavenie Tokenu do stavu, v akom je dodávaný výrobcom (stav "*unissued*"). Technicky sa jedná o vykonanie prechodu "*unissue*" životného cyklu Tokenu, popísaného v katalógovom liste [1]. Deinicializáciu Tokenu obvykle realizuje bezpečnostný správca organizácie, ktorý disponuje prístupovým heslom *Administrátora* Tokenu *APW*. Aby mohol byť Token deinicializovaný, musí byť v stave "*issued*". *Administrátor* zrealizuje deinicializáciu Tokenu stlačením tlačidla *Unissue*. Ak *Administrátor* nebol doposiaľ autentifikovaný, je požiadaný o vloženie hesla *APW*.

Upozornenie: deinicializácia Tokenu nevratne zmaže všetky údaje v užívateľskej pamäti Tokenu, vrátane kľúčov v RSA bunkách a údajov v oblastiach MEM !

Poznámka: po úspešnej deinicializácii Tokenu je prístupové heslo Administrátora APW nastavené na výrobcom preddefinovanú náhradnú hodnotu "admin".

---

4 Dokumentácia

[1] GNT USB Token - dátový list, SoftIdea, s.r.o. , Máj 2011, http://www.softidea.sk/gnt_datasheet_sk.pdf

[2] SIPKCS - Aplikačné programové rozhranie PKCS#11 pre GNT USB Token, SoftIdea, s.r.o. , Máj 2011, http://www.softidea.sk/sipkcs_specification_sk.pdf

[3] PKCS #11 v2.20: Cryptographic Token Interface Standard, RSA Laboratories, June 2004, http://www.rsasecurity.com

SoftIdea s.r.o.
Sliačska 10, 831 02 Bratislava
tel.: +421 2 444 60 444
fax.: +421 2 446 40 441
http://www.softidea.sk
info@softidea.sk