GNT USB Token

Viacfaktorová autentizácia

Šifrovanie e-mailov, elektronický podpis, šifrovanie disku

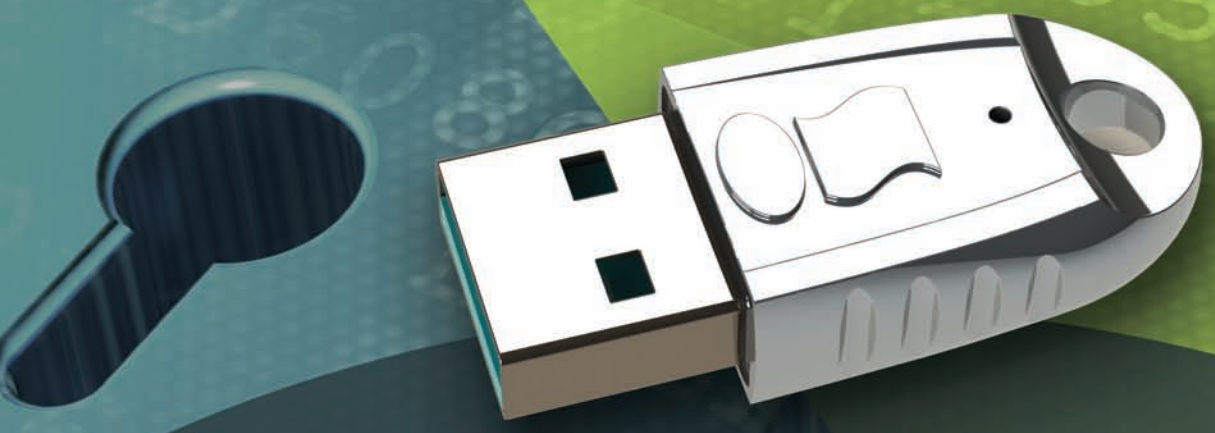
Ochrana a licencovanie hardvéru a softvéru

Spracovávanie citlivých a klasifikovaných dát

Systémy na správu dokumentov s riadením prístupu (DRM)

Podporuje PGP, Thunderbird, Firefox, VeraCrypt, OpenVPN

e-Government



Unikátne sériové číslo

Počítadlo nesprávnych pokusov o prihlásenie

RSA generácia kľúčových párov do 4096 bit

128 bit AES, 64 bit DES, 192 bit Triple DES, SHA-1, SHA-256

Generátor náhodných čísel (FIPS 140-2)

Opatrenia proti spätnej analýze

34,5 KB bezpečnej užívateľskej pamäte

Uchovanie dát min. 10 rokov a 500 000 zapisovacích cyklov

Kompatibilné s PKCS #11 štandardom

Odolné kovové púzdro, LED indikujúca aktivitu

Common Criteria EAL 4+ ready

amset

Tel.: +421-2-44460444 | amset@amset.sk | www.amset.sk

SOFTIDEA

GNT USB Token

dátový list

November 2018

Obsah

Zoznam tabuliek

1 Všeobecný popis

GNT USB Token (ďalej i Token) je hardvérové kryptografické zariadenie s rozhraním *USB 2.0 "Full Speed"* vykonávajúce kryptografické operácie so zameraním na šifrovanie, elektronický podpis a kontrolu integrity dát. Šifrovanie zamedzuje prístup neautorizovanej osoby a elektronický podpis jednoznačne identifikuje pôvodcu elektronického dokumentu. Kontrola integrity umožňuje detegovať dodatočné zmeny v dokumente.

Jadrom Tokenu je hardvérový výpočtový systém špeciálne navrhnutý pre zabezpečenie extrémne vysokej ochrany údajov. Sú prítomné viaceré aktívne ochranné systémy implementované na úrovni architektúry integrovaného obvodu. V Tokene je implementované symetrické aj asymetrické šifrovanie, výpočet hodnoty hašu a generovanie sekvencií náhodných čísel. Kryptografické operácie sú implementované priamo vo firmvéri Tokenu. Pre najvyššiu úroveň bezpečnosti je možné systém konfigurovať tak, že citlivé údajové štruktúry (napríklad súkromné kryptografické kľúče) nie je možné z Tokenu nijakým spôsobom extrahovať.

Token môže byť použitý ako nositeľ digitálnej identifikácie majiteľa Tokenu. Identifikácia je založená na priradení kľúčového páru verejného a súkromného kľúča ku konkrétnemu užívateľovi, pričom toto priradenie je potvrdené certifikačnou autoritou. Verejný kľúč umožňuje šifrovať správy určené majiteľovi Tokenu a overiť platnosť ním vygenerovaných elektronických podpisov. Súkromný kľúč umožňuje majiteľovi Tokenu podpisovať dokumenty elektronickým podpisom a dešifrovať jemu určené šifrované správy. Základným predpokladom bezpečnosti systému je bezpečné uloženie súkromného kľúča. Prístup k operáciám so súkromným kľúčom uloženým v Tokene je chránený 128 bitovým heslom. Pri konfigurácii na najvyššiu úroveň bezpečnosti súkromný kľúč nikdy neopustí hardvér Tokenu. Po vygenerovaní kľúčového páru je možné po zadaní hesla vykonávať kryptografické operácie so súkromným kľúčom (podpisovať a dešifrovať dokumenty), ale nie je možné získať samotný súkromný kľúč. Tieto skutočnosti umožňujú využitie Tokenu pre dvojfaktorovú autentifikáciu, kde majiteľ súkromného kľúča potvrdzuje svoju identitu vlastníctvom Tokenu (ktorý je jediným možným fyzickým nositeľom súkromného kľúča) a zároveň znalosťou prihlasovacieho hesla. Získanie prístupu len k jednému z uvedených faktorov (napríklad krádežou Tokenu, alebo odpozeraním prístupového hesla) neumožňuje vykonávať kryptografické operácie so súkromným kľúčom.

Token je kompaktný, ľahký, vodotesný a má dobrú mechanickú odolnosť vďaka kovovému puzdru. Svetlo emitujúca dióda umiestnená na Tokene blikaním indikuje činnosť Tokenu.

2 Kryptografické mechanizmy

Token podporuje nasledujúce kryptografické mechanizmy. Všetky podporované kryptografické mechanizmy sú úplne implementované na úrovni firmvéru Tokenu:

- Asymetrický šifrovací algoritmus **RSA s dĺžkou kľúča 2048 bitov.**
- Tri symetrické šifrovacie algoritmy: **AES s dĺžkou kľúča 128 bitov**, **DES s dĺžkou kľúča 64 bitov a triple DES s dĺžkou kľúča 192 bitov**.
- Štyri módy pre symetrické šifrovanie, dva blokové: **CBC**, **ECB** a dva prúdové: **CTR**, **OFB**.
- Dva hašovacie algoritmy: **SHA-1**, **SHA-256**.
- Generátor náhodných čísiel.

2.1 Súlad so štandardami

Mechanizmus	Štandardy
RSA generovanie kľúča	PKCS #11 v2.20 (CKM_RSA_PKCS_KEY_PAIR_GEN)
RSA šifrovanie/dešifrovanie	PKCS #1 v1.5 (RSAES-PKCS1-v1_5), X.509, ISO/IEC 9594-8 PKCS #11 v2.20 (CKM_RSA_PKCS, CKM_RSA_X_509)
RSA generovanie / overovanie elektronického podpisu	PKCS #1 v1.5 (RSASSA-PKCS1-v1_5) X.509, ISO/IEC 9594-8 PKCS #11 v2.20 (CKM_RSA_PKCS, CKM_SHA1_RSA_PKCS, CKM_SHA256_RSA_PKCS, CKM_RSA_X_509)
SHA-1, SHA-256	FIPS 180-2 PKCS #11 v2.20 (CKM_SHA_1, CKM_SHA256)
Generovanie náhodných čísel	FIPS 140-1
AES	FIPS 197 PKCS #11 v2.20 (CKM_AES_KEY_GEN, CKM_AES_ECB, CKM_AES_CBC_PAD) PKCS #11 v2.30 (CKM_AES_OFB, CKM_AES_CTR)
DES	FIPS 46-3 PKCS #11 v2.20 (CKM_DES_KEY_GEN, CKM_DES_ECB, CKM_DES_CBC_PAD, CKM_DES_OFB8)
triple DES	FIPS 46-3 PKCS #11 v2.20 (CKM_DES3_KEY_GEN, CKM_DES3_ECB, CKM_DES3_CBC_PAD)
Padding pre CBC mód AES, DES, 3DES	PKCS #7
ECB,CBC, OFB módy pre symetrické algoritmy	FIPS 81
CTR mód pre symetrické algoritmy	ATM Security Specification v1.1

Tabuľka 1: Štandardy kryptografických mechanizmov

3 Kryptografické operácie

Operačné jadro Tokenu je navrhnuté tak, aby bolo schopné realizovať väčšinu štandardných protokolov informačnej bezpečnosti založených na symetrickom a asymetrickom šifrovaní a na ich kombinácii. Token podporuje nasledujúce kryptografické operácie a ich kombinácie:

- Generovanie sekvencie náhodných čísel,
- generovanie RSA kľúčového páru,
- ukladanie citlivých dát v chránenej permanentnej pamäti,
- výpočet hašu,
- generovanie elektronického podpisu,
- overenie elektronického podpisu,
- šifrovanie a dešifrovanie správ asymetrickou šifrou,
- šifrovanie a dešifrovanie správ symetrickou šifrou,
- simultánne symetrické šifrovanie správy a generovanie digitálneho podpisu,
- simultánne symetrické dešifrovanie a overovanie digitálneho podpisu,
- simultánny import šifrovaného symetrického kľúča, jeho dešifrovanie a dešifrovanie správy,
- simultánne šifrovanie správy a export symetrického šifrovacieho kľúča zašifrovaného asymetrickou šifrou.

Generovanie RSA kľúčového páru trvá obvykle menej ako 20s, avšak zo štatistickej povahy tejto operácie vyplýva, že môže trvať i dlhšie. Počas tejto doby je LED dióda Tokenu zhasnutá.

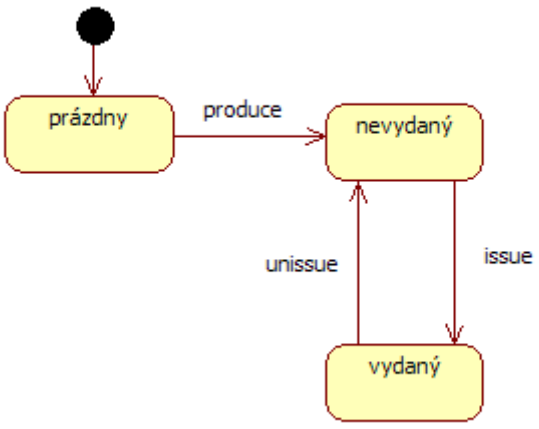
4 Bezpečnostné funkcie

- Bezpečné úložisko. Prístup k dátam a kryptografickým funkciám Tokenu je chránený prístupovými heslami PIN1 a PIN2 dĺžky 128 bitov (resp. 16 Bytov). Pomocou PIN1 a PIN2 je možné zadefinovať rôznu úroveň ochrany prístupu k dátam.
- Generovanie RSA kľúčového páru prebieha priamo v Tokene.
- Token je možné konfigurovať tak, že súkromná časť RSA kľúčového páru nikdy neopustí hardvér Tokenu.
- Počítadlo neúspešných prihlásení. Po *N* neúspešných prihláseniach, sa automaticky zničia všetky dáta uložené v Tokene a Token sa vráti do výrobného stavu. Parameter *N* je nastavený počas inicializácie Tokenu administrátorom. Nastavením *N=0* administrátor deaktivuje túto funkciu.
- Súčasťou vnoreného systému Tokenu je pamäť typu EEPROM, integrovaná do čipu Tokenu. Obsah pamäte je šifrovaný na úrovni čipu.

- RSA kľúče sú uložené v pamäti Tokenu v špeciálne chránenej zóne. Každý RSA kľúč je umiestnený v tzv. RSA bunke. Pri inicializácii Tokenu je možné špecifikovať povolené spôsoby použitia RSA kľúča v konkrétnej bunke, ako napríklad šifrovanie, alebo generovanie elektronického podpisu. Je možné zadefinovať, či RSA kľúč je do / z danej bunky možné importovať / exportovať, generovať a či je možné ho mazať. Ak je niektorá RSA bunka pri inicializácii nastavená ako neexportovateľná, nie je možné žiadnym spôsobom exportovať kľúč z danej RSA bunky mimo hardvér Tokenu. To platí aj pre užívateľa prihláseného do Tokenu.
- Ochrana pred útokmi SPA (Simple Power Analysis) a DPA (Differential Power Analysis); SPA a DPA sú založené na meraní spotreby elektrického prúdu počas používania Tokenu.
- Ochrana pred útokmi napäťovým a frekvenčným monitoringom. Ak Token zaznamená kolísanie napätia alebo frekvencie oscilátora mimo definovaný rozsah, okamžite zastaví vykonávanie aktuálnej inštrukcie a vygeneruje reset procesora. Zároveň dôjde k automatickému odhláseniu užívateľa z Tokenu. Táto bezpečnostná funkcia je implementovaná priamo v čipe Tokenu a zabraňuje nežiadúcej manipulácii s dátami v Tokene.
- Prihlasovanie sa do Tokenu je odolné voči časovaciemu útoku (timing attack). Procedúra prihlasovania trvá vždy rovnaký čas bez ohľadu na to, koľko správnych, alebo nesprávnych znakov hesla bolo zadaných.
- V čipe Tokenu sú implementované špeciálne vrstvové štruktúry na znemožnenie sledovania toku dát na internej zbernici čipu. Dátové a adresné vodiče sú ukryté pod aktívnou kovovou vrstvou.
- Token je najmodernejšími metódami chránený proti spätnému inžinierstvu.

5 Životný cyklus

Na obrázku č. 1 je zobrazený stavový diagram životného cyklu Tokenu. Popis stavov je v nasledujúcej tabuľke. Prechod *produce* vykoná výrobca po autentifikácii heslom výrobcu PPW.



Obrázok 1: Životný cyklus Tokenu

Prechod *issue* predstavuje inicializáciu Tokenu a vykoná ho *Administrátor.* Prechod *unissue* môže vykonať *Administrátor, Výrobca,* alebo k nemu dôjde automaticky, po prekročení limitu na počet nesprávnych prihlásení.

Upozornenie: Prechod unissue nenávratne zmaže všetky užívateľské dáta a konfigurácie !

Stav	Popis
prázdny	Token je v tomto stave po opustení výrobnej linky. Nemá zadefinované žiadne objekty v pamäti, ani sériové číslo.
nevydaný	Náhradné heslo *Administrátora* APW je zadefinované, sériové číslo je nastavené. Token neobsahuje žiadne užívateľské dáta. Token v tomto stave umožňuje len: prihlásenie *Administrátora*, nastavenie hesla Administrátora, prechod od stavu "vydaný". Každý pokus zavolať inú funkciu skončí chybou. V tomto stave je Token nepoužiteľný pre *Užívateľa*.
vydaný	Prístupové heslá PIN1 a PIN2 sú nastavené, veľkosti a prístupové práva pre MEM1/2/3 sú zadefinované, atribúty RSA kľúčov sú zadefinované. Token je inicializovaný a plne funkčný.

Tabuľka 2: Zoznam možných stavov Tokenu

6 Vnútorná štruktúra

6.1 Pamäť

Interná pamäť Tokenu má veľkosť 36kB. Z toho firmvér využíva 1536B pre systémové dáta a pre nultú RSA bunku, ktorá je vždy prítomná a má fixné atribúty. Zvyšných 35328B označených ako „Užívateľská pamäť“ je určených pre dáta užívateľa. Logická schéma užívateľskej pamäti je v nasledujúcej tabuľke:

Užívateľská pamäť						
35328 B						
RSA bunky				MEM oblasti		
RSA bunka 1	RSA bunka 2	RSA bunka 3	...	MEM1	MEM2	MEM3

Tabuľka 3: Štruktúra užívateľskej pamäti

Užívateľská pamäť je konfigurovateľná *Administrátorom* počas inicializácie. *Administrátor* definuje počas inicializácie nasledujúce parametre:

- počet RSA buniek (úložísk pre RSA kľúče) v rozsahu 0 - 32. Každá RSA bunka zaberá 544 B užívateľskej pamäti.
- Atribúty jednotlivých RSA buniek (pozri kapitolu 6.2RSA bunky).
- Počet pamäťových oblastí MEM v rozsahu 0 - 3.
- Veľkosť jednotlivých pamäťových oblastí MEM. Veľkosť je obmedzená len dostupnou voľnou užívateľskou pamäťou.
- Prístupové práva k jednotlivým MEM oblastiam (pozri kapitolu 6.3MEM oblasti).

6.2 RSA bunky

RSA kľúčové páry sú uložené v pamäti v tzv. RSA bunkách. RSA bunka je úložisko verejného aj súkromného RSA kľúča, a určuje ich atribúty. Počet RSA buniek je voliteľný. Token podporuje do 32 konfigurovateľných RSA buniek a ich presný počet a atribúty sú definované *Administrátorom* počas inicializácie. Samotný RSA kľúč sa do bunky dostáva buď vygenerovaním priamo v Tokene alebo importovaním existujúceho kľúča cez USB rozhranie. Popri konfigurovateľných RSA bunkách je k dispozícii aj špeciálna nekonfigurovateľná RSA bunka 0 s fixnými atribútmi. Logická schéma RSA buniek je v nasledujúcej tabuľke:

RSA bunky				
bunka 0	bunka 1	bunka 2	bunka 3	...
fixné atribúty	konfigurovateľné atribúty	konfigurovateľné atribúty	konfigurovateľné atribúty	konfigurovateľné atribúty

Tabuľka 4: Štruktúra RSA buniek

- **RSA bunka 0**: je určená pre RSA kľúčový pár s fixnými atribútmi. Fixné nastavenie atribútov je definované v nasledujúcej tabuľke. Táto bunka je prístupná cez PIN1 aj PIN2, je umiestnená v systémovej pamäti Tokenu, mimo užívateľskej pamäti a je v Tokene vždy prítomná.
- **RSA bunky 1-32**: sú určené pre RSA kľúčové páry s konfigurovateľnými atribútmi. Význam jednotlivých atribútov je vysvetlený v nasledujúcej tabuľke. Každá z RSA buniek má vlastné nastavenie atribútov.

Atribút RSA bunky	Popis	RSA bunka 0
exportovateľný	Ak je nastavený, kompletný RSA kľúč (vrátane súkromného kľúča) je možné z bunky exportovať mimo Token.	nie
importovateľný	Ak je nastavený, kompletný RSA kľúč (vrátane súkromného kľúča) je možné do bunky importovať.	áno
generovateľný	Ak je nastavený, je možné interne v bunke vygenerovať RSA kľúč.	áno
exportovateľný len počas generovania	Ak je nastavený, kompletný RSA kľúč je možné exportovať mimo Token počas generovania kľúča a len počas generovania kľúča: 1. Kľúč je vygenerovaný v RAM pamäti čipu. 2. Kľúč je exportovaný z RAM pamäte mimo Token. 3. Kľúč je skopírovaný z RAM pamäte do príslušnej RSA bunky a automaticky je označený ako neexportovateľný. 4. Kľúč je zmazaný z RAM pamäte.	nie
zmazateľný	Ak je nastavený, RSA kľúč môže byť z bunky zmazaný.	áno
prístupný na PIN1	Ak je nastavený, *Užívateľ* môže používať tento kľúč na	áno

Atribút RSA bunky	Popis	RSA bunka 0
	RSA operácie po zadaní správneho PIN1 hesla.	
prístupný na PIN2	Ak je nastavený, *Užívateľ* môže používať tento kľúč na RSA operácie po zadaní správneho PIN2 hesla.	áno
šifrovanie / dešifrovanie správy	Ak je nastavený, kľúč môže byť použitý na šifrovanie/dešifrovanie správ.	áno
generovanie / overovanie digitálneho podpisu	Ak je nastavený, kľúč môže byť použitý na generovanie / overovanie digitálneho podpisu.	áno
šifrovanie / dešifrovanie symetrického kľúča	Ak je nastavený, kľúč môže byť použitý na šifrovanie/dešifrovanie tajného symetrického kľúča.	áno

Tabuľka 5: Atribúty RSA buniek

Poznámka: Užívateľ nemá možnosť konfiguráciu RSA buniek meniť. Po inicializácii nie je možné meniť počet ani atribúty RSA buniek. Zmena sa dá dosiahnuť len reinicializáciou (pozri kapitolu 5 Životný cyklus), čo je spojené so stratou všetkých užívateľských dát a nastavení.

6.3 MEM oblasti

Každá MEM oblasť Tokenu reprezentujú dátové úložisko pre citlivé údaje *Užívateľa* s presne definovanými prístupovými právami. Počet MEM oblastí je voliteľný v rozsahu 0-3. Prístupové práva k jednotlivým MEM oblastiam zahŕňajú.

- úroveň autentifikácie *Užívateľa* požadovanú pre zápis a mazanie oblasti
- úroveň autentifikácie *Užívateľa* požadovanú pre čítanie z oblasti

Prístupové práva zadefinuje *Administrátor* počas inicializácie Tokenu doplnením požadovanej úrovne autentifikácie do nasledujúcej tabuľky zvlášť pre každú inicializovanú MEM oblasť:

Poznámka: Na mazanie údajov z danej MEM oblasti sa vyžaduje rovnaká úroveň autentifikácie ako na zápis.

Prístupové práva k MEM oblastiam				
MEM oblasť	-	voľne prístupné	PIN1 prístupné	PIN2 prístupné
MEM1	čítanie			
	zápis			
MEM2	čítanie			
	zápis			
MEM3	čítanie			
	zápis			

Tabuľka 6: Prístupové práva k MEM oblastiam

Poznámka: Užívateľ nemá možnosť konfiguráciu MEM oblastí meniť. Po inicializácii nie je možné meniť veľkosť ani prístupové práva MEM oblastí. Zmena sa dá dosiahnuť len reinicializáciou (pozri kapitolu 5 Životný cyklus), čo je spojené so stratou všetkých užívateľských dát a nastavení !

7 Politika prístupu

7.1 Užívatelia

Token rozlišuje tri typy autentifikovaných užívateľov, ktorí môžu vykonávať operácie s Tokenom – výrobca Tokenu (*Výrobca*), bezpečnostný správca (*Administrátor*) a konečný užívateľ (*Užívateľ*). *Administrátor* je osoba, zodpovedná za inicializáciu a konfiguráciu Tokenu. *Užívateľ* je osoba, používajúca Token na ochranu svojich dát a/alebo na preukázanie svojej identity.

Prístupové práva *Výrobcu* sú obmedzené len na uloženie nasledujúcich výrobných dát do Tokenu:

- jedinečné sériové číslo Tokenu,
- prvotné prístupové heslo pre *Administrátora*.

Výrobca môže tiež vykonať prechod *unissue* (pozri kapitolu 5 Životný cyklus). Sériové číslo nie je po nastavení možné zmeniť. *Výrobca* nemá prístup ku kryptografickým operáciám ani k dátam uloženým v Tokene.

Administrátor môže len inicializovať a konfigurovať Token, ale nemá prístup ku kryptografickým operáciám ani k dátam uloženým v Tokene. Úlohou *Administrátora* je definovať bezpečnostnú politiku Tokenu v kontexte jeho plánovaného použitia. To znamená napríklad definovať počet RSA buniek v Tokene a prístupové práva k nim, definovať prístupové práva pre MEM oblasti a nastaviť dočasné prístupové heslá (PIN1 a PIN2) pre *Užívateľa*.

Užívateľ môže vykonávať všetky kryptografické operácie s Tokenom v súlade s konfiguráciou definovanou *Administrátorom* a pristupovať k dátam uloženým v MEM oblastiach, pre ktoré disponuje príslušnými prístupovými právami, ale nemôže Token inicializovať ani konfigurovať. Aby mohol *Užívateľ* používať Token, musí ho *Administrátor* najprv inicializovať.

7.2 Autentifikácia a správa hesiel

Dáta uložené v MEM oblastiach Tokenu a kryptografické operácie sú prístupné len po úspešnej autentifikácii *Užívateľa*, po správnom zadaní prístupového hesla. To zabraňuje nežiadúcemu prístupu neautorizovaných osôb k dátam *Užívateľa*. Prístupové heslá majú dĺžku 128 bitov (16 znakov); využitie všetkých 128 bitov prakticky znemožňuje použitie útoku hrubou silou na odhalenie hesla. Autentifikačný systém je chránený proti časovému útoku – procedúra overenia prístupového hesla trvá za každých okolností rovnaký čas, nezávisle od správnosti zadaného hesla.

Autentifikácia *Užívateľa* má dve úrovne rozlíšené dvomi heslami PIN1 a PIN2. Táto skutočnosť sa dá využiť napríklad pre vertikálne rozčlenenie prístupu ku kryptografickým operáciám pre vyššie zabezpečenie najcitlivejších údajových štruktúr. Typickým príkladom môže byť zadefinovanie

PIN1 prístupného RSA kľúča len pre šifrovanie a dešifrovanie správ a druhého, PIN2 prístupného RSA kľúča len pre elektronický podpis. *Administrátor* pri inicializácii definuje, ktoré zdroje Tokenu sú prístupné po autentifikácii na úroveň PIN1 a ktoré na PIN2.

Prvotné heslo *Administrátora* nastavuje *Výrobca* počas prechodu *produce,* prvotné heslá *Užívateľa* PIN1 a PIN2 nastavuje *Administrátor* počas prechodu *issue* (pozri kapitolu 5 Životný cyklus). Prvotné heslá sú dočasné a je potrebné ich pred začatím používania Tokenu zmeniť.

Pre zmenu prístupových hesiel inicializovaného Tokenu platia nasledujúce pravidlá: Heslo *Administrátora* APW sa dá zmeniť len po autentifikácii na úroveň aktuálneho APW. PIN2 sa dá zmeniť len po autentifikácii na úroveň PIN2. PIN1 je možné zmeniť po autentifikácii na úroveň PIN1 alebo PIN2. Uvedená skutočnosť umožňuje využitie hesla PIN2 ako "odblokovacieho" hesla pre prípad straty PIN1. Úplný zoznam možností zmeny hesiel je v nasledujúcej tabuľke:

Úroveň autentifikácie potrebná na zmenu hesla	
Heslo	**Úroveň autentifikácie**
PIN1	aktuálne PIN1
	PIN2
	APW [1]
PIN2	aktuálne PIN2
	APW [1]
APW	aktuálne APW
	PPW [2]

Tabuľka 7: Úroveň autentifikácie potrebná na zmenu hesla

[1)] len v rámci prechodu *issue*, pozri kap. 5Životný cyklus

[2)] len v rámci prechodu *produce*, alebo *unissue* pozri kap. 5Životný cyklus

Po autentifikácii *Administrátora* heslom APW, alebo po autentifikácii *Výrobcu* heslom PPW je možné vykonaním prechodu *unissue* uviesť Token do stavu "nevydaný", kedy sú všetky užívateľské dáta zmazané a APW sa zmení späť na náhradnú hodnotu nastavenú *Výrobcom* v rámci prechodu *produce*.

8 Aplikačné programové rozhranie

Token je štandardne dodávaný s aplikačným rozhraním SIPKCS [2], ktoré implementuje štandard PKCS #11 vyvinutý RSA Security Inc. [3]. Súčasťou dodávky je inicializačný program GINIT [1]. Pre vývoj na platforme riadeného prostredia .NET je dostupný PKCS #11 adaptér pre .NET. Špeciálne požiadavky konzultujte s výrobcom SoftIdea s.r.o. .

9 Aplikačné možnosti

Token je určený pre využitie v aplikáciách vyžadujúcich veľmi vysokú úroveň informačnej bezpečnosti. Vďaka svojej konštrukcii je vhodný ako osobný autentifikačný a prístupový prostriedok v sieťach mobilných účastníkov. Oblasť použitia Tokenu zahŕňa napríklad nasledujúce aplikácie:

- Komunikačné aplikácie s požiadavkou na ochranu pred odpočúvaním.
- Informačné siete s požiadavkou na autentifikáciu účastníkov siete.
- Vnútropodnikové komunikačné systémy.
- Systémy na správu dokumentov s riadením prístupu.
- Systémy na ochranu softvéru pred pirátstvom.
- Systémy s elektronickým podpisom.
- Licenčné a kreditné systémy.

10 Dokumentácia

[1] GINIT - užívateľský manuál, SoftIdea, s.r.o. , May 2011, http://www.softidea.sk/ginit_manual_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 2/D, 831 02 Bratislava
tel.: +421 2 444 60 444
fax.: +421 2 446 40 441
http://www.softidea.sk
info@softidea.sk