

APSD-Klient

Návod na obsluhu

Rev. 1.1

29.07.2013

OBSAH

1.	Úvod.....	2
2.	Špecifikácia APSD kľúčenky.....	2
3.	Určenie.....	2
4.	Systémové požiadavky.....	3
5.	Opis stavových LED diód <i>APSD kľúčenky</i>	3
6.	Použitie softvérovej aplikácie <i>APSD-Klient</i>	3
7.	Autentifikácia používateľa.....	4
8.	Šifrovanie dát.....	5
9.	Dešifrovanie dát.....	6
10.	Riešenie problémov.....	8

1. Úvod

ALISON Portable Security Device (APSD) je prostriedok šifrovej ochrany informácií určený predovšetkým na zabezpečenú výmenu elektronických dokumentov a súborov s využitím hardvérových tokenov označovaných ako *APSD klúčenky* a softvérovej aplikácie označovanej ako *APSD-Klient*.

Tento dokument opisuje spôsob používania *APSD klúčeniek* v súčinnosti s PC, na ktorom je nainštalovaná softvérová aplikácia *APSD-Klient*.

2. Špecifikácia APSD klúčenky

Zariadenie



Opis

- Dvojfaktorová autentizácia = heslo + biometria
- Biometrická identifikácia (odtlačkom prsta)
- Chránené (šifrované) úložisko

Ďalšia špecifikácia:

- Šifrovací algoritmus Advanced Encryption Standard (AES), 256-bit, mód cipher-block chaining (CBC)
- Kryptografický procesor testovaný podľa FIPS 140-2 na Level 3
- Kapacity EEPROM od 2GB až do 64GB
- LED status - napájanie, dátová aktivita, autentifikácia

2. Určenie

Prostriedok šifrovej ochrany informácií APSD je určený na šifrovanie elektronických súborov s možnosťou uloženia zašifrovaných súborov na personálnom počítači alebo na *APSD klúčenke*, na bezpečnú úschovu elektronických súborov a na zabezpečený prenos súborov.

Šifrovanie elektronických súborov prebieha s použitím softvérovej aplikácie *APSD-Klient* a *APSD klúčenky*, pričom samotný proces šifrovania prebieha priamo v *APSD klúčenke*. Šifrovací kľúč danej skupiny používateľov je do *APSD klúčenky* uložený pri jej inicializácii administrátorom, a to pomocou aplikácie *APSD-KMC*. Po zašifrovaní určeného súboru, nachádzajúceho sa v originálnej otvorenej podobe na pracovnej stanici, dôjde k automatickému zmazaniu originálu a k vytvoreniu a uloženiu zašifrovaného súboru, tzn. dáta na konci šifrovacieho procesu zostávajú len v jednej - zašifrovanej podobe. Dešifrovanie zašifrovaných súborov je možné len s použitím softvérovej aplikácie *APSD-Klient* a *APSD klúčenky*, resp. *APSD klúčeniek*, ktoré majú rovnaký šifrovací kľúč, to znamená patria spoločnej skupine používateľov. Skupiny používateľov sú zadefinované administrátorom APSD v aplikácii *APSD-KMC*.

Na úschovu a prenos dokumentov je k dispozícii šifrované úložisko na *APSD klúčenke*. Toto úložisko je dostupné až po autentifikácii používateľa heslom a odtlačkom prsta v aplikácii *APSD-Klient*. Pre prácu s týmto úložiskom musí byť na určenom PC vopred nainštalovaná aplikácia *APSD-Klient*, ktorá beží na pozadí od štartu daného PC. *APSD klúčenka* chráni dáta na úložisku prostredníctvom AES (Advanced Encryption Standard) algoritmu. Dáta sú automaticky šifrované a dešifrované počas ich prenosu z/na *APSD klúčenku*.

3. Systémové požiadavky Hardvérové

požiadavky

- personálny počítač (PC) s min. 1x USB port typ A

Operačný systém

- Microsoft Windows XP Professional SP2 alebo SP3
- Microsoft Windows 7

Operačný systém s podporou USB 2.0 /1.1 Mass Storage Devices

2. Opis stavových LED diód APSD klúčienky

APSD klúčienky sú vybavené dvoma LED diódami indikujúcimi ich operačný status.

Stav	Opis
Zelené svetlo stále.	APSD klúčienka je odomknutá - používateľ sa autentifikoval.
Zelené svetlo prerušované. Frekvencia blikania je približne 1 sek.	Pripravenosť APSD klúčienky na autentifikáciu používateľa odtlačkom prsta.
Zelené svetlo prerušované. Frekvencia blikania je viac ako 1 sek., pomalé blikanie.	Pripravenosť APSD klúčienky na autentifikáciu používateľa odtlačkom prsta, ak zariadenie nebolo autentifikované dlhšiu dobu od pripojenia k PC (idle).
Červené svetlo, bliknutie.	Zlyhanie autentifikácie užívateľa odtlačkom prsta. Zariadenie sa vráti do stavu Pripravenosť APSD klúčienky na autentifikáciu používateľa odtlačkom prsta.
Červené svetlo prerušované. Frekvencia blikania je približne 1 sek.	APSD klúčienka sa načítava po pripojení k PC. Tento stav trvá krátku dobu a APSD klúčienka po načítaní prejde do stavu pripravenosti na autentifikáciu používateľa. Ak je tento stav trvalý, APSD klúčienka je úplne blokována a je potrebné ju obnoviť systémovou recykláciou administrátorom pomocou aplikácie APSD-KMC.
Červené svetlo stále.	APSD klúčienka je zamknutá.
Modré svetlo.	Indikuje prenos dát na /z APSD klúčienky.
Prerušované modré a červené svetlo.	APSD klúčienka nemá platný / kompatibilný firmware.

3. Použitie softvérovej aplikácie APSD-Klient

Program APSD-Klient, resp. Apsd.exe, je predinštalovaný na danom PC (pracovnej stanici). Po štarte PC je spustený automaticky ako systémová služba - stav spustenia je indikovaný na obrazovke v stavovom riadku.



Avšak v závislosti od Operačného módu práce prostriedku APSD, môže aplikácia *APSD-Klient* automaticky štartovať len pod definovaným používateľským profilom.

V prípade, ak sa aplikácia automaticky nespustí, alebo sa počas práce s PC z úmyselných alebo neúmyselných dôvodov jej činnosť ukončí, je ju možné spustiť manuálne z miesta na Vašom počítači, kde bola nainštalovaná. V takom prípade vyhľadajte aplikáciu na Vašom počítači, napríklad pri štandardnom postupe bude nainštalovaná v adresári *Apsd*,

cesta C: > Program Files > Apsd > Apsd.exe

resp. My Computer > Disk C: > Program Files > Apsd > Apsd.exe

a spustíte ju dvojklikom na súbor *Apsd.exe*.

Spustené aplikácie signalizuje ikona na spodnej lište obrazovky.



Autentifikácia používateľa

Používateľ zasunie *APSD kľúčenku* do USB portu určeného PC.

Po zasunutí *APSD kľúčenky* sa zobrazí žiadosť o zadanie hesla používateľa pre prístup do zariadenia.

LED dióda na *APSD kľúčenke* svieti na červeno.



Po zadaní hesla sa zobrazí požiadavka o autentifikáciu používateľa odtlačkom prsta.

LED dióda na *APSD kľúčenke* bliká na zeleno, čo signalizuje pripravenosť *APSD kľúčenky* na autentifikáciu používateľa odtlačkom prsta.



Ak je autentifikácia používateľa úspešná, LED dióda na *APSD kľúčenke* svieti stálym zeleným svetlom, čo indikuje, že *APSD kľúčenka* je odomknutá - používateľ sa autentifikoval.

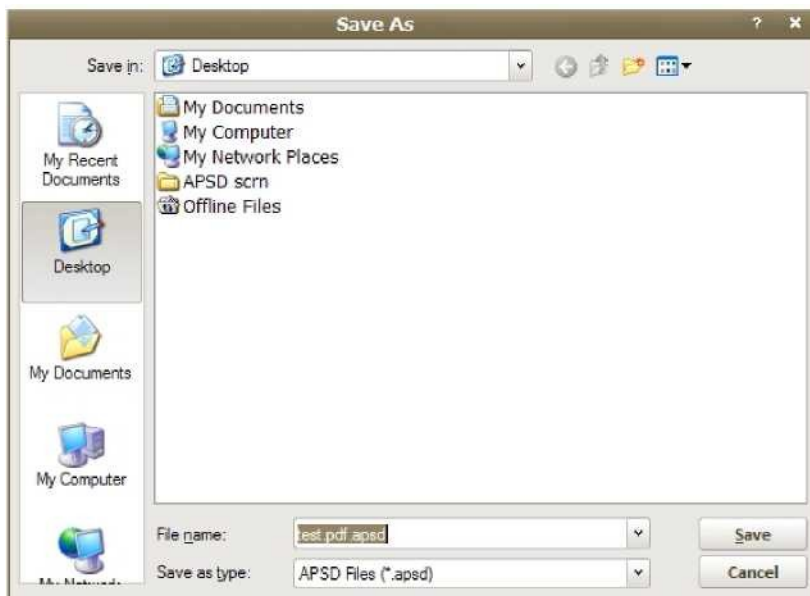
7. Šifrovanie dát



Po úspešnej autentifikácii používateľa je prístupná funkcia šifrovania dát a možnosť ich ukladania na šifrovanom úložisku *APSD kľúčenky*.

Kliknite pravým tlačidlom myši na súbor, ktorý chcete zašifrovať. Zobrazí sa menu, kde jednou z voliteľných funkcií, ktoré môžete aplikovať na daný súbor, je aj funkcia „Zašifrovať“.

Po potvrdení voľby „Zašifrovať“ sa objaví výzva na uloženie súboru, ktorý vznikne po zašifrovaní. Názov súboru zostáva zachovaný aj s pôvodnou príponou, za ktorú je pridaná prípona „.apsd“.



Po potvrdení názvu a miesta uloženia zašifrovaného súboru, prebehne šifrovanie. Po zašifrovaní dát dôjde k automatickému zmazaniu originálu, tzn. dáta zostávajú len v jednej - zašifrovanej podobe.

Po úspešnom ukončení šifrovania sa zobrazí potvrdzujúca správa.

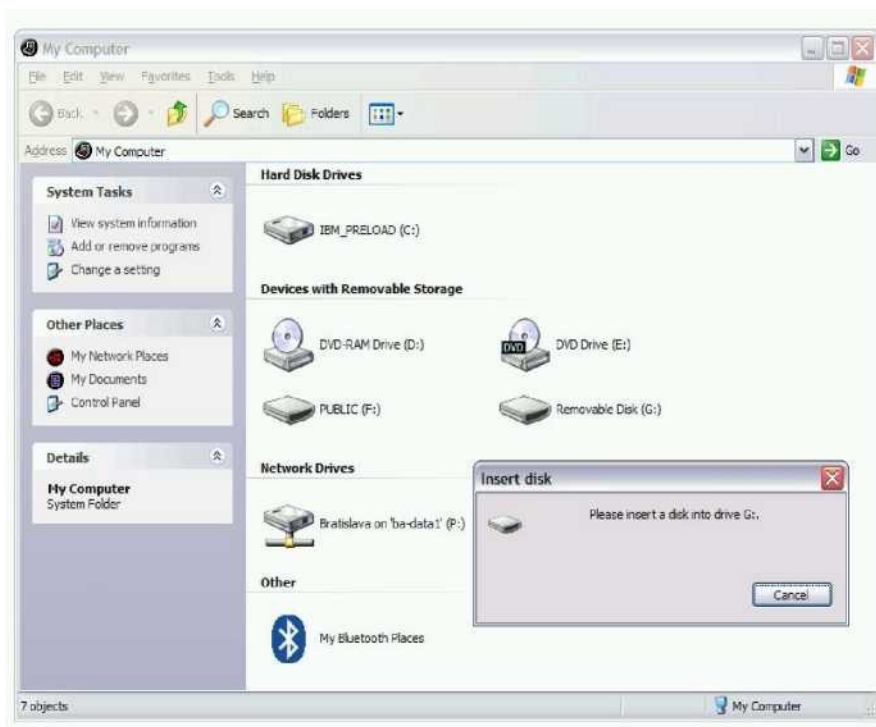


Pozn.: Pokiaľ je súbor uložený na CD/DVD médiu alebo médiu bez možnosti zápisu, nie je možné ho zašifrovať. V takomto prípade je potrebné súbor pred šifrovaním presunúť napr. na PC alebo na chránené úložisko *APSD kľúčanky*.

Zašifrovaný súbor je možné prenášať na zabezpečenom úložisku *APSD kľúčanky* alebo môže zostať uložený na danom PC (pracovnej stanici) a následne odoslaný emailom, prípadne prenášaný na inom médiu.

Dáta uložené na zabezpečenom úložisku *APSD kľúčanky* sú viditeľné len pre používateľa, ktorý sa autentifikoval pomocou aplikácie *APSD-Klient*. Sú dešifrované automaticky pri ich otvorení autentifikovaným používateľom.

Ak je *APSD kľúčanka* zamknutá (používateľ sa neautentifikoval), ale používateľ sa pokúša sa o prístup na šifrované úložisko, objaví sa hláška „Vložte disk do mechaniky G:“ - kde G predstavuje označenie mechaniky priradené *APSD kľúčanke*.

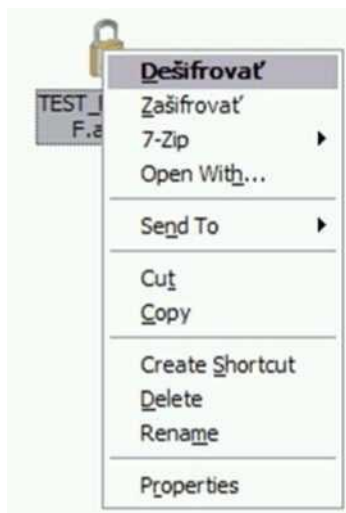


8. Dešifrovanie dát

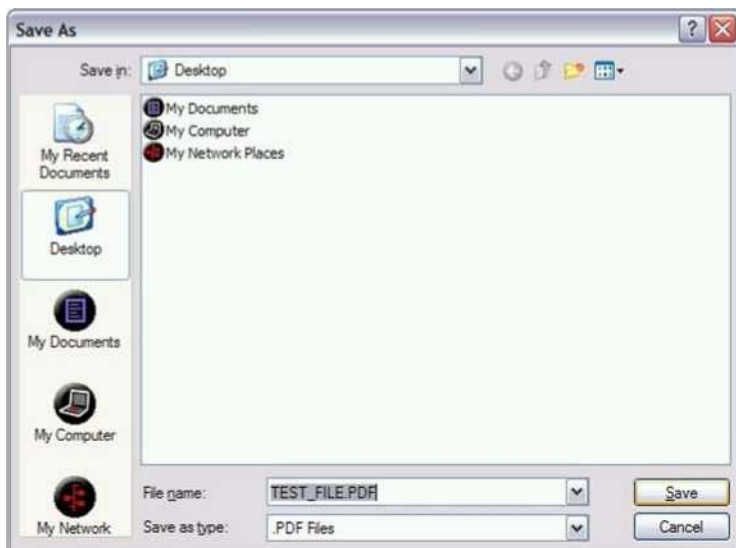
Na dešifrovanie dát je potrebný autentifikovaný používateľ v aplikácii APSD-Klient tej istej skupiny ako používateľ, ktorý dáta zašifroval.

Po autentifikovaní v aplikácii APSD-Klient kliknite pravým tlačidlom myši na zašifrovaný súbor.

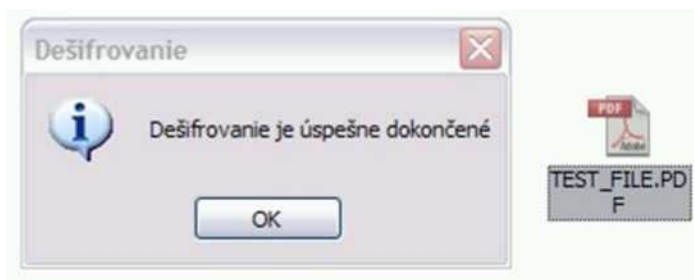
Zobrazí sa menu, kde jednou z voliteľných funkcií, ktoré môžete aplikovať na daný súbor je aj funkcia „Dešifrovať“



Po potvrdení voľby „Dešifrovať“ sa objaví výzva na uloženie súboru, ktorý vznikne po dešifrovaní.



Po úspešnom dešifrovaní sa zobrazí potvrdzujúca hláška.



Zašifrovaný súbor sa odstráni z pôvodného miesta.

Pozn.: Pokiaľ je súbor uložený na CD/DVD médiu alebo médiu bez možnosti zápisu, nie je možné ho šifrovať / dešifrovať. V takomto prípade je potrebné súbor pred šifrovaním/dešifrovaním presunúť napr. na chránené úložisko APSD kľúčanky.



9. Riešenie problémov

- Problém

Hláška „Nemáte zapnutý program Apsd“.



Toto hlásenie sa zobrazí pri pokuse o zašifrovanie súboru v prípade, že nie je spustený program *Apsd.exe*.

Riešenie

Je potrebné spustiť program *Apsd.exe*. Postup spustenia je opísaný v časti 6. *Použitie softvérovej aplikácie APSD-Klient*.

- Problém

Hláška „Zlyhanie oneskoreného zápisu“

Počas ukladania alebo premiestňovania dokumentov alebo manipulácii so súbormi v systéme Windows XP sa môžu opakovane zobrazovať chybové hlásenia oznamujúce zlyhanie oneskoreného zápisu.



Tento problém sa môže vyskytnúť, ak je pre disk zapnutá funkcia ukladania zápisu na disku do vyrovnávacej pamäte. V prípade rýchleho výberu APSD kľúčanky z USB portu hneď po transfere dát sa môže zobrazit' toto hlásenie.

Riešenie

Odpájanie APSD kľúčanky z USB portu je potrebné vykonať kliknutím na ikonu "Bezpečné odstránenie hardwaru" na systémovej lište v prostredí MS Windows (v prípade neúspechu aj opakovane 2-3 krát) a následným odstránením zariadenia z ponuky.

Ikona „Bezpečné odstránenie hardwaru“:

Safely-Remove Hardware

Zoznam/ponuka pripojených zariadení pre výber APSD kľúčkenky:

