CRYPTO MEMORIJE

UVOD

- Gubitak kako prijenosnih uređaja tako i podataka je postala svakodnevnica
- 92 % svih kompanija u Europi je barem jednom izgubila prijenosno računalo i podatke iz raznih razloga
- Računalo je lako zamijeniti ali je problem u podacima koji su nestali i koji su nezaštićeni

UVOD

- Vrlo je bitna svijest rizika i opasnosti koje mogu donijeti svi podaci koji nisu zaštićeni

NAJVAŽNIJI KRITERIJI ZA SIGURAN PRIJENOS I POHRANU PODATAKA

- Enkripcija – prikladan izbor enkripcije je bitan za sigurnost podataka
- Za visoke standarde sigurnosti podataka preporučeno je koristiti barem AES enkripciju sa ključem dužine 256 bita

NAJVAŽNIJI KRITERIJI ZA SIGURAN PRIJENOS I POHRANU PODATAKA

- Kontrola pristupa –može varirati od jednostavne lozinke do kompleksnih autentifikacijskih metoda sa više faktora
- Kompleksna pristupna metoda sa dva faktora autentifikacije (pametna kartica i PIN) nudi vrlo visoku razinu zaštite podataka

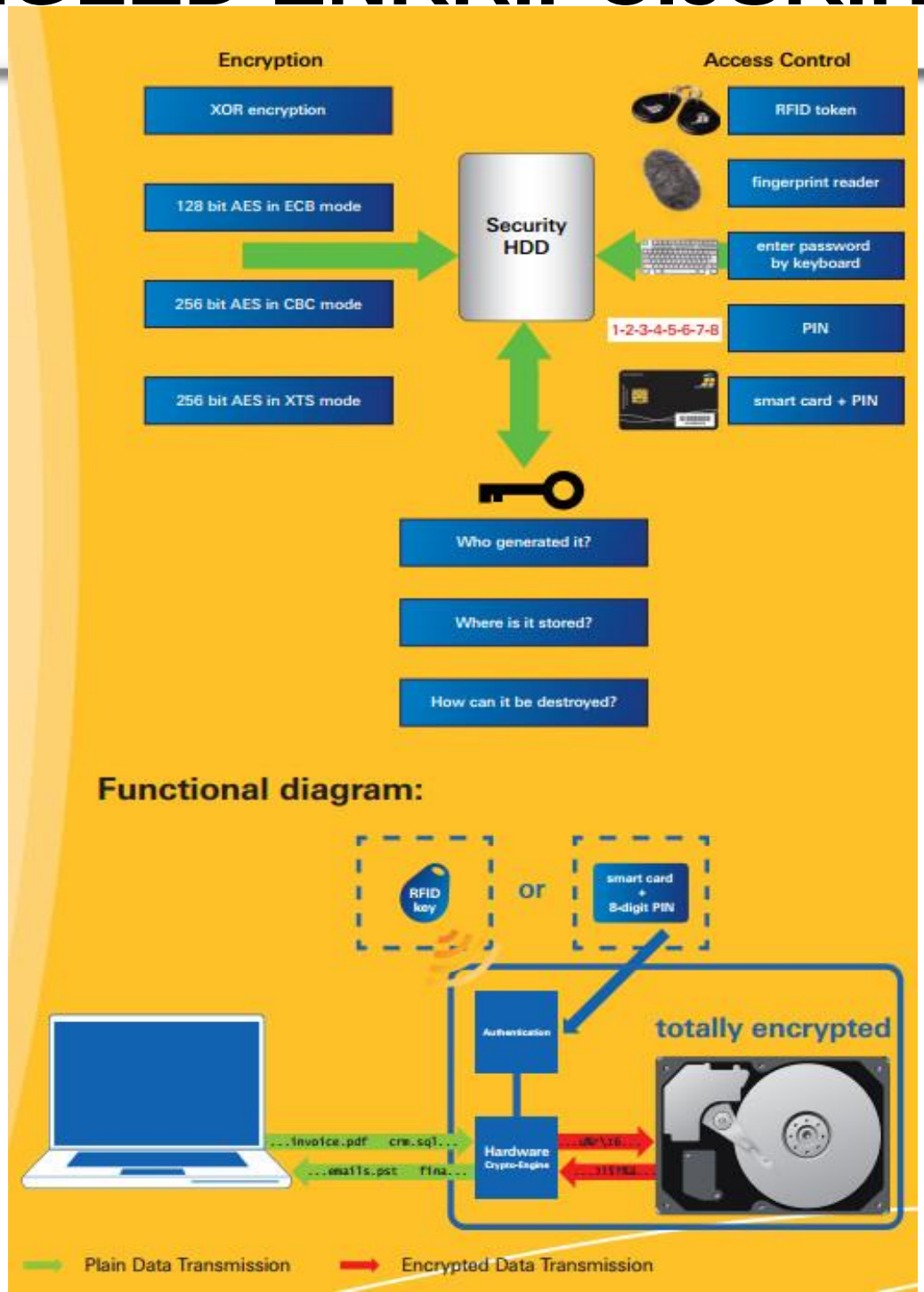
NAJVAŽNIJI KRITERIJI ZA SIGURAN PRIJENOS I POHRANU PODATAKA

- Administracija kriptografskog ključa – bitno je znati kako je ključ proizveden, gdje i kako pospremljen
- Treba znati da li ključ može biti uništen ako je potrebno
- Kod najsigurnijih proizvoda ključ je pospremljen tako da ga korisnik može generirati, promjeniti i uništiti

NAJVAŽNIJI KRITERIJI ZA SIGURAN PRIJENOS I POHRANU PODATAKA

- Sigurnosni uređaj za pohranjivanje i zaštitu podataka mora sadržavati sva 3 sigurnosna kriterija
- Sigurnosni kriteriji – enkripcija, kotrola pristupa i administriranje kriptografskog ključa
- Ako jedan kriterij nije zadovoljen cijeli sigurnosni lanac ne podlježe maksimalnom stupnju sigurnosti

PREGLED ENKRIPCIJSKIH SUSTAVA



UREĐAJI ZA SIGURNU POHRANU

- Široki spektar kriptiranih proizvoda od 2GB do 2TB

USB SIGURNOSNI STICK USS256

- Kontrola pristupa zaštićena lozinkom
- 256 bitna AES enkripcija
- Kriptografski ključ je u kodiranoj flash memoriji
- Zaštićen kućištem od vlage i udaraca te manipulacija
- Samo određivanje broja pogrešnih lozinki od 1 do maksimalno 256 unosa što svaki korisnik definira sam za sebe
- Automatsko brisanje podataka ako je prekoračen broj krivih unosa lozinke
- Dodatna sigurnost za korištenje na različitim računalima
- “plug & play” za sve Windows OS
- Kompatibilno sa USB 1.1 i 2.0

USS256

- Autentifikacija unosom lozinke
- Nakon pogrešnog unosa lozinke preko dozvoljenog broja automatski se vraća na tvorničke postavke te su podaci automatski izbrisani
- Zaštita osjetljivih podataka na visokoj razini

RFID SIGURNOSNI HDD/SSD RS64

- RFID (radio frekvencijska identifikacija) kontrola pristupa
- XOR hardverska enkripcija cijelog diska
- Pametno zaključavanje HDD-a (aktivacija ATA lozinke)
- Kriptografski ključ u kriptiranom HDD-u
- Nemogućnost pristupa podacima na disku bez jednog od dva uključena RFID ključa

RFID SIGURNOSNI HDD/SSD RS64

- Automatsko zaključavanje HDD-a odmah nakon isključivanja iz računala
- Svi podaci su automatski kodirani hardverskim enkripcijskim modulom u realnom vremenu
- Bootabilan
- Neovisan o OS-u
- Kompatibilan sa USB 1.1 i 2.0
- 320 GB, 500 GB, 640 GB, 750 GB, 1TB i 2TB kao HDD
- 120 GB, 240, 500 GB kao SSD

RFID SIGURNOSNI HDD/SSD RS64

- Svi podaci zaštićeni od neovlaštenog pristupa sa enkripcijom podataka, pametnim zaključavanjem (ATA lozinka) i RFID kontrolom pristupa
- Pruža korisnicima visoku razinu zaštite

Designed for Windows®
Certification Capable

Mac™ OS

RoHS COMPLIANT

RFID SIGURNOSNI HDD/SSD RS128

- RFID (radio frekvencijska identifikacija) kontrola pristupa
- 128 bitna hardverska enkripcija cijelog diska
- Kriptografski ključ u kriptiranom HDD
- Nemogućnost pristupa podacima bez jednog od dva RFID ključa
- Automatsko zaključavanje nakon isključivanja iz računala
- Svi spremljeni podaci su automatski kodirani hardverskom enkripcijom u realnom vremenu

RFID SIGURNOSNI HDD/SSD RS128

- Bootabilan i neovisan o operacijskom sustavu
- Kompatibilan sa USB 1.1 i 2.0
- Mini USB i integrirani USB konektor
- 320GB, 500GB, 640GB, 750GB , 1TB i 2TB kao HDD
- 120GB, 240GB, 500 GBkao SSD
- Pouzdano štiti osjetljive podatke od neželjenih pogleda
- Svaki sektor na disku koristi dodatni različiti enkripcijski vektor

RFID SIGURNOSNI HDD/SSD RS256

- RFID (radio frekvencijska identifikacija) kontrola pristupa
- 256 bitna hardverska enkripcija cijelog diska
- AES ključ pospremljen na HDD
- Nemogućnost pristupa HDD bez jednog od dva RFID ključa
- Automatsko kodiranje HDD prilikom uklanjanja iz računala

RFID SIGURNOSNI HDD/SSD RS256

- Svi spremljeni podaci su automatski kodirani hardverskom enkripcijom u realnom vremenu
- Silikonski anti šok protektori
- Aluminijsko robusno kućište
- Bootabilan i neovisan o OS
- Kompatibilan sa USB 3.0 i 2.0
- 320GB, 500GB, 750GB, 1TB i 2TB kao HDD
- 120GB, 240GB i 500GB kao SSD

RFID SIGURNOSNI HDD/SSD RS256

- Sigurno rješenje za korisnike
- Otporan na mehaničke utjecaje i elektromagnetske valove
- Kriptiranje podataka u realnom vremenu

Designed for Windows®
Certification Capable

Mac OS

linux os

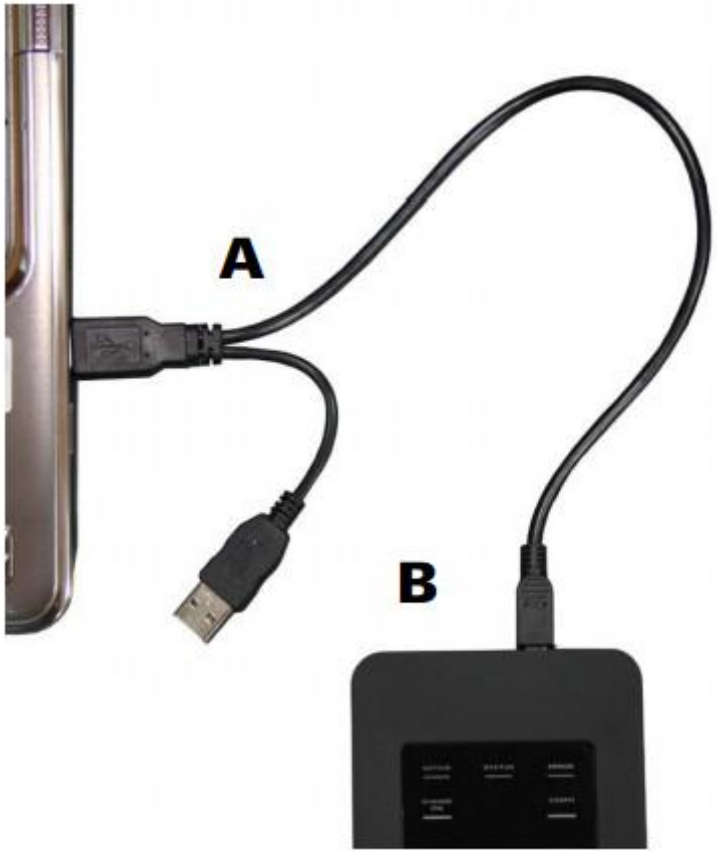
TVRDI DISK VISOKE SIGURNOSTI HS128 I HS256

- Profesionalno rješenje
- Autentifikacija sa dva faktora – pametna kartica 8 znamenkasti PIN
- Certificirana hardverska enkripcija za HS128 , AES 128 bitnom enkripcijom u ECB modu dok za HS256 , AES 256 bitnom enkripcijom u CBC modu
- Kriptografski ključ se nalazi na pametnoj kartici

TVRDI DISK VISOKE SIGURNOSTI HS128 I HS256

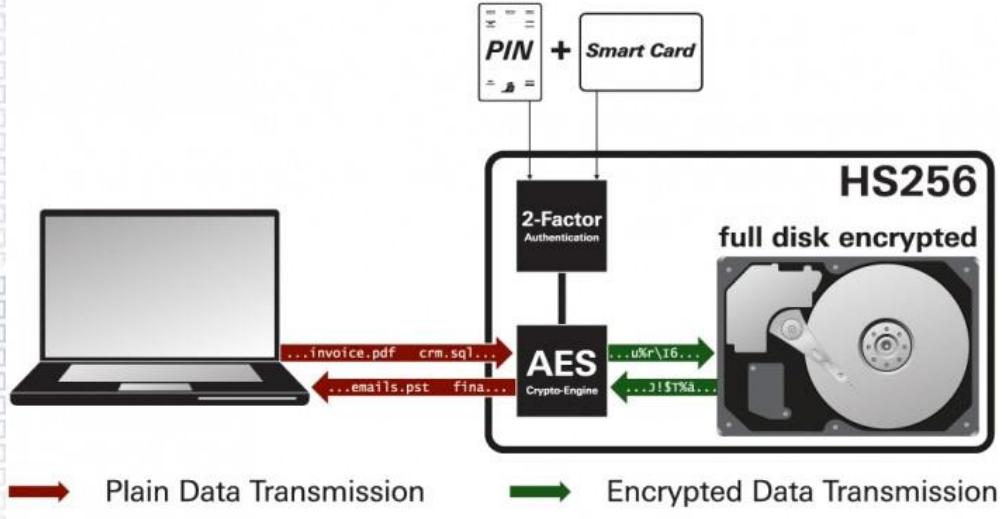
- Zaštita pristupa pametnoj kartici 8 znamenkastim pinom
- Metodu enkripcije certificirao NIST: FIPS 197
- NIST – National Institute of Standards and Technology (SAD)
- Svi podaci spremljeni i automatski enkriptirani hardverskom enkripcijom u realnom vremenu
- Automatsko kodiranje nakon isključivanja iz računala

TVRDI DISK VISOKE SIGURNOSTI HS128 I HS256



- Bootabilan i neovisan o OS
- Kompatibilan sa USB 1.1 i 2.0
- 320 GB, 500GB, 640GB, 750GB, 1TB i 2TB kao HDD
- 120GB, 240 GB i 500GB kao SSD

TVRDI DISK VISOKE SIGURNOSTI HS128 I HS256



- Dva faktora autentifikacije za pristup podacima
- Znati i imati princip
- Imati – posjedovanje pametne kartice sa odgovarajućim kriptografskim ključem, potvrda dolazi umetanjem kartice u HDD
- Znati – korisnik mora znati 8 znamenkasti PIN uz autoriziranu pametnu karticu, potvrda dolazi unosom 8 znamenkastog PIN-a

TVRDI DISK VISOKE SIGURNOSTI HS128 I HS256

- U slučaju manipulacije pametna kartica će biti nepovratno uništena i onemogućena te je pristup podacima nemoguć
- Ako je disk uspješno otključan podaci se razmjenjuje poput normalnog tvrdog diska
- Nema dodatnih programa
- Maksimalan stupanj sigurnosti

AES 256 BIT ENCRYPTION
SECURITY EDITION

TVRDI DISK VISOKE SIGURNOSTI HS256S

- Profesionalno rješenje najveće kategorije i stupnja zaštite
- Pruža mogućnost administracije kriptografskog ključa od strane korisnika
- Generiranje, mjenjanje, kopiranje, uništavanje
- Certificiran od strane NIST-a i BSI-a
- NIST – National Institute of Standards and Technology (SAD)
- BSI – German Federal Office for Information Security

TVRDI DISK VISOKE SIGURNOSTI HS256S

- Zaštita pristupa pametnom karticom i 8 znamenkastim pinom
- NIST : FIPS 197 certifikat za enkripcijsku metodu
- Pametna kartica certificirana sa FIPS 140-2 Level 3
- Bootabilan i neovisan o OS
- Kompatibilan sa USB 1.1 i USB 2.0
- 500GB, 1TB i 2TB kao HDD i 120GB, 240GB, 512GB kao SSD

TVRDI DISK VISOKE SIGURNOSTI HS256S

- Zaštita podataka, projekata, financija, projekata, računovodstva, razvoja i sl. protiv neovlaštenog pristupa
- Podaci su sigurni ako se disk zagubi
- 3 sigurnosna mehanizma – enkripcija, kontrola pristupa, administracija ključa

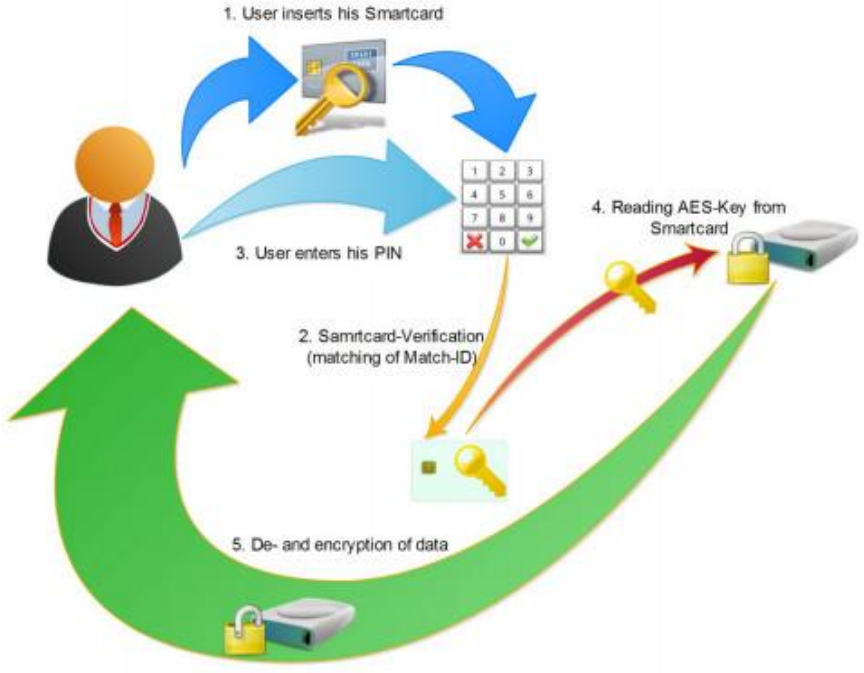
EUROPRISE European Privacy Seal

Privacy at its best.

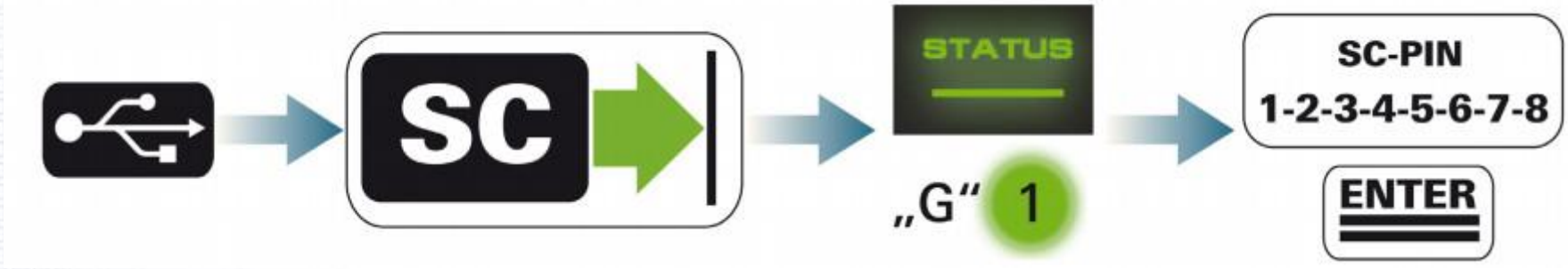
TVRDI DISK VISOKE SIGURNOSTI HS256S

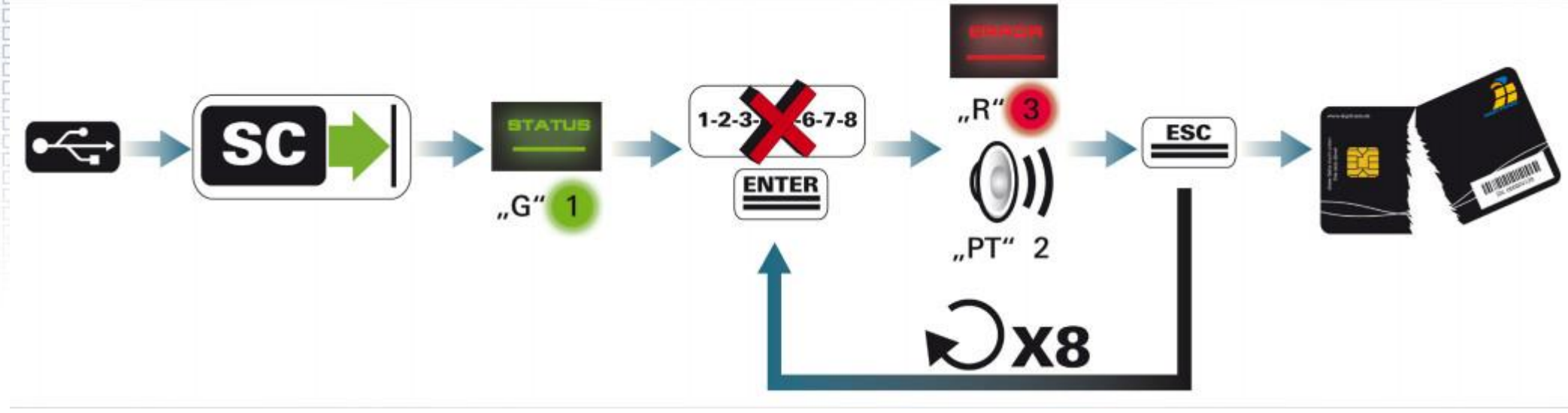
- Mogućnost generiranja, promjene , kopiranja ili u hitnom slučaju poništavanja enkripcijskog ključa
- Kriptografski ključ je pospremljen kodiran na pametnoj kartici
- Odvojen od zaštićenih i kodiranih podataka

12. Data flow:

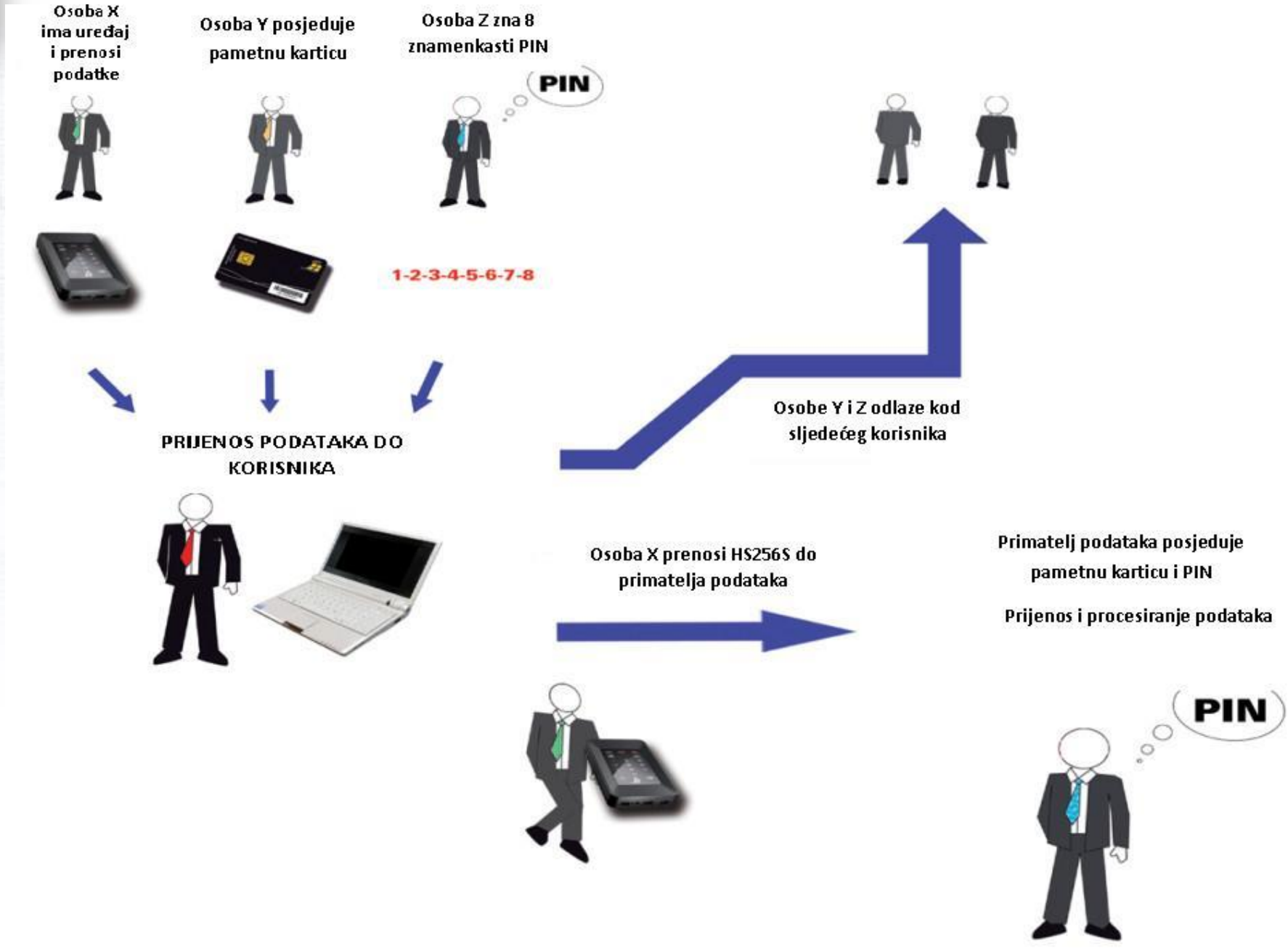


TVRDI DISK VISOKE SIGURNOSTI HS256S



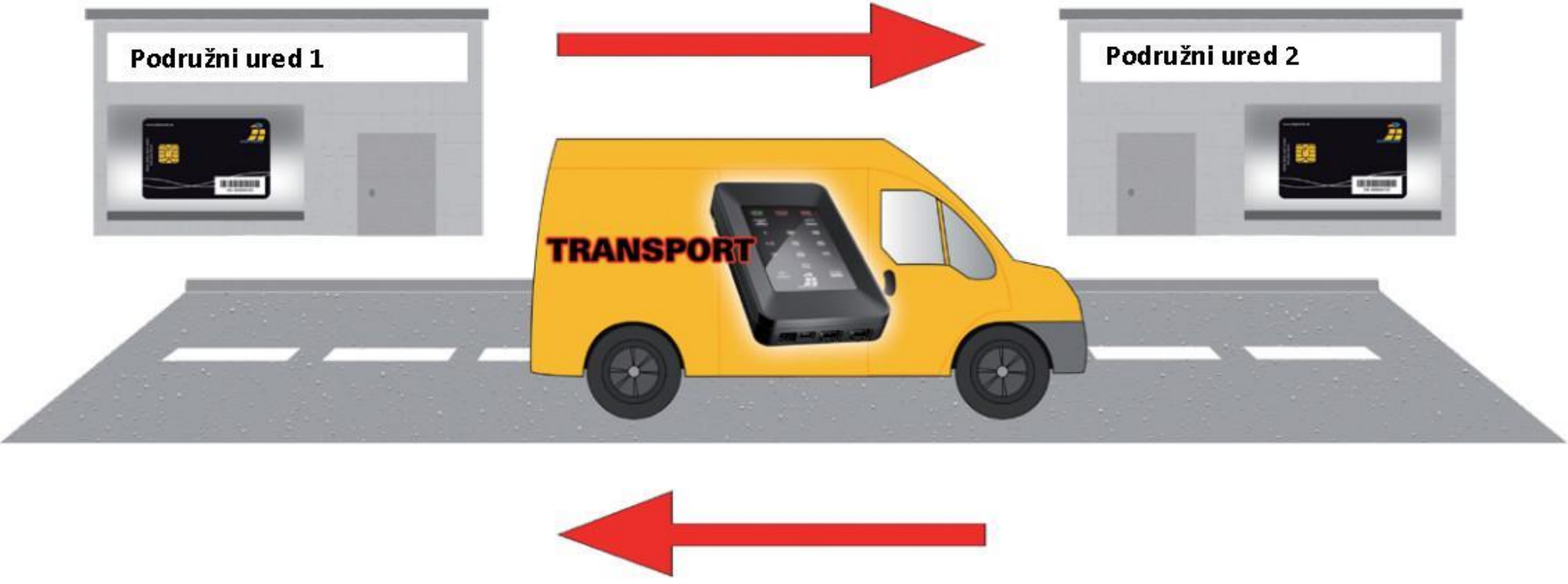


PRIMJENA

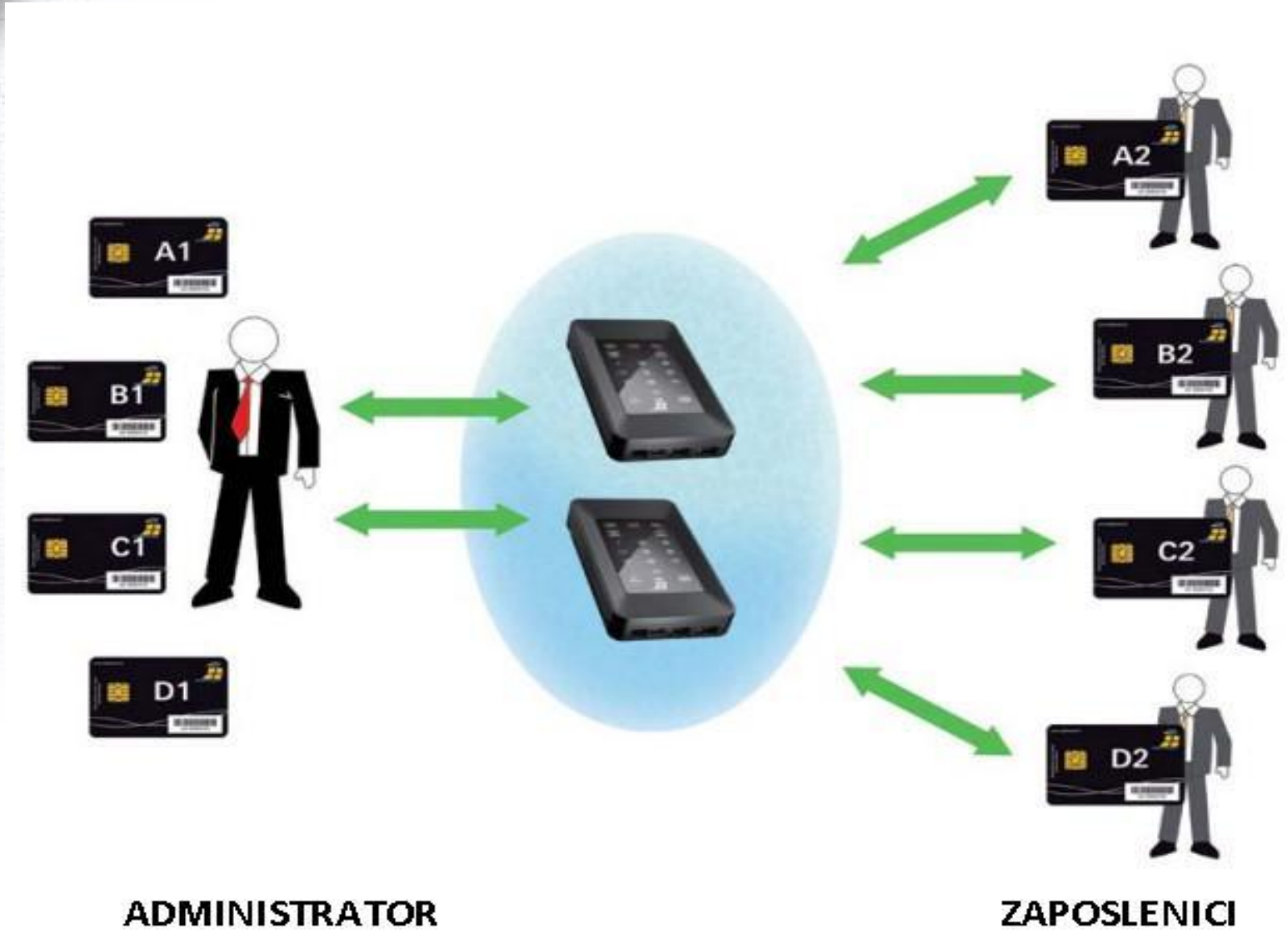

Osoba X ima uređaj i prenosi podatke
Osoba Y posjeduje pametnu karticu
Osoba Z zna 8 znamenkasti PIN
PIN
1-2-3-4-5-6-7-8
PRIJENOS PODATAKA DO KORISNIKA
Osobe Y i Z odlaze kod sljedećeg korisnika
Osoba X prenosi HS256S do primatelja podataka
Primatelj podataka posjeduje pametnu karticu i PIN
Prijenos i procesiranje podataka
PIN

PRIMJENA

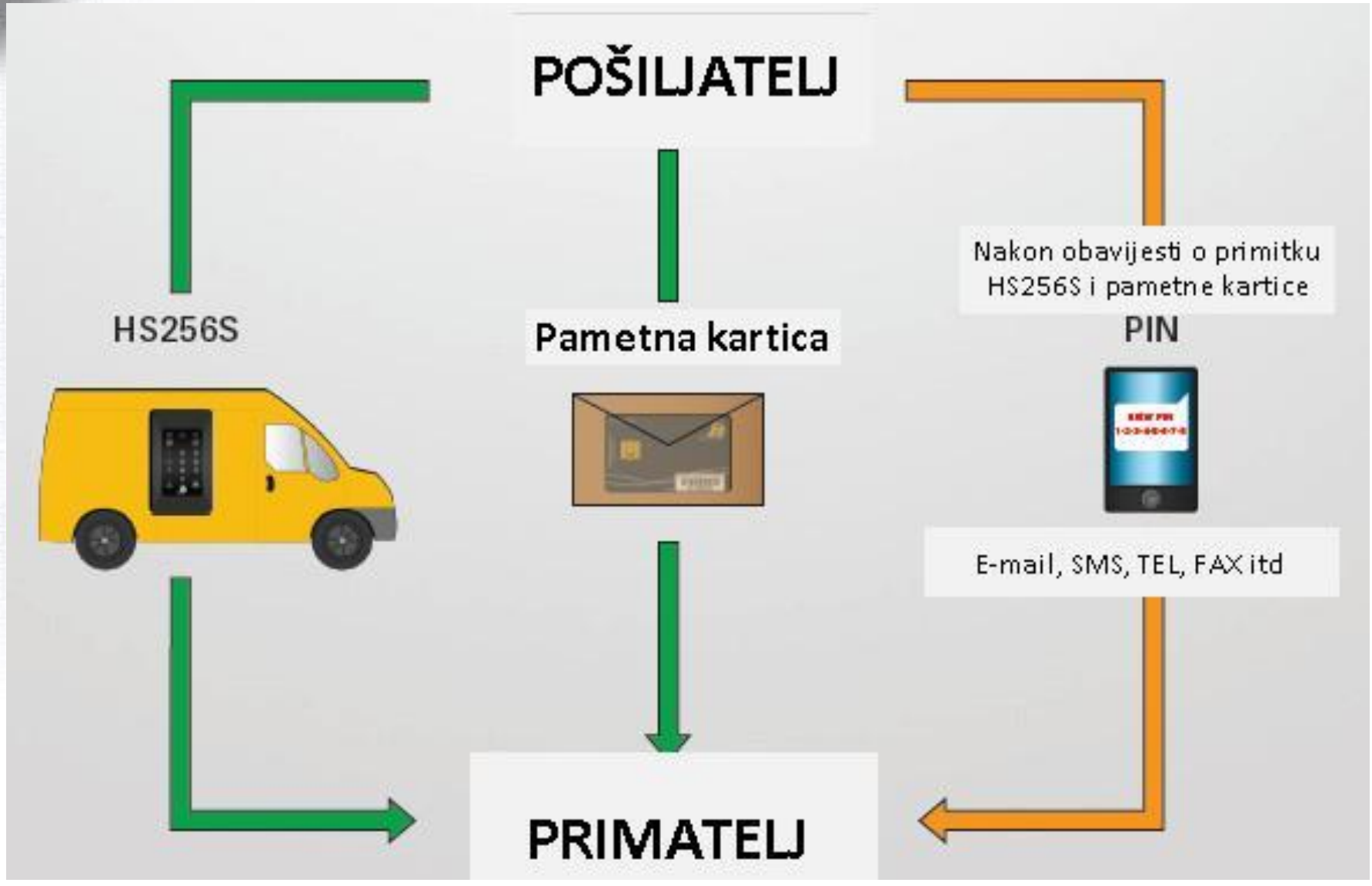
Oba podružna ureda imaju jednu ili više pametnih kartica sa vlastitim kriptografskim ključem



PRIMJENA



PRIMJENA

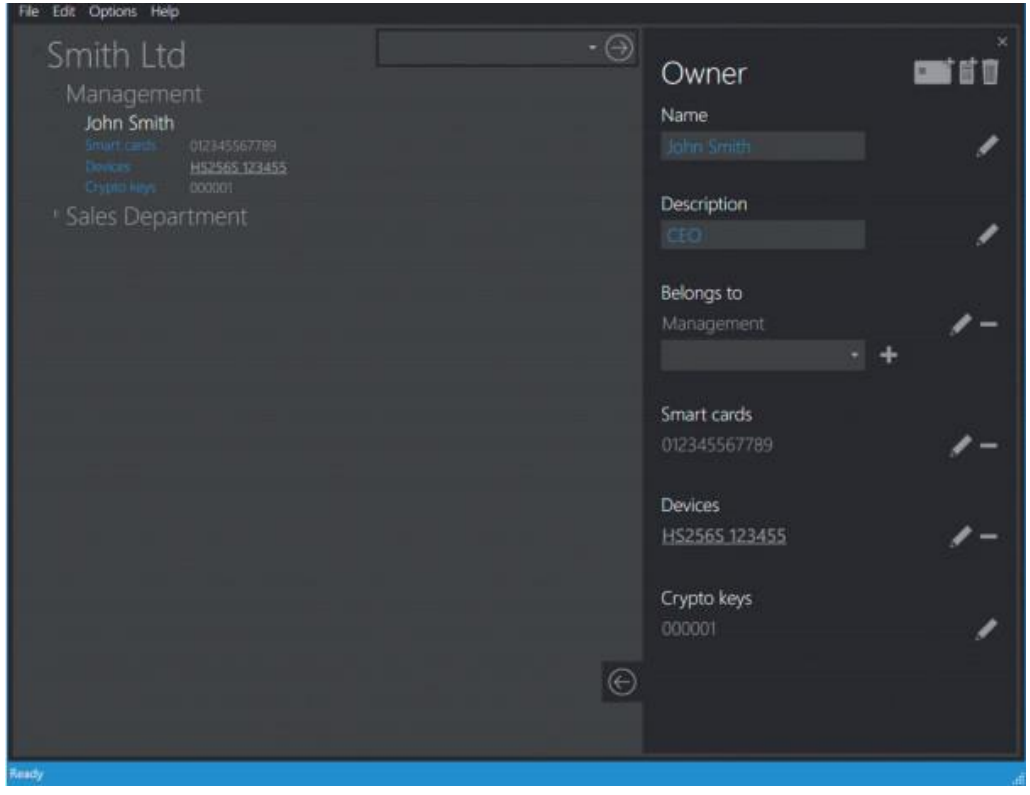

POŠILJATELJ
HS256S
Pametna kartica
Nakon obavijesti o primitku HS256S i pametne kartice
PIN
E-mail, SMS, TEL, FAX itd
PRIMATELJ

PRIMJENA

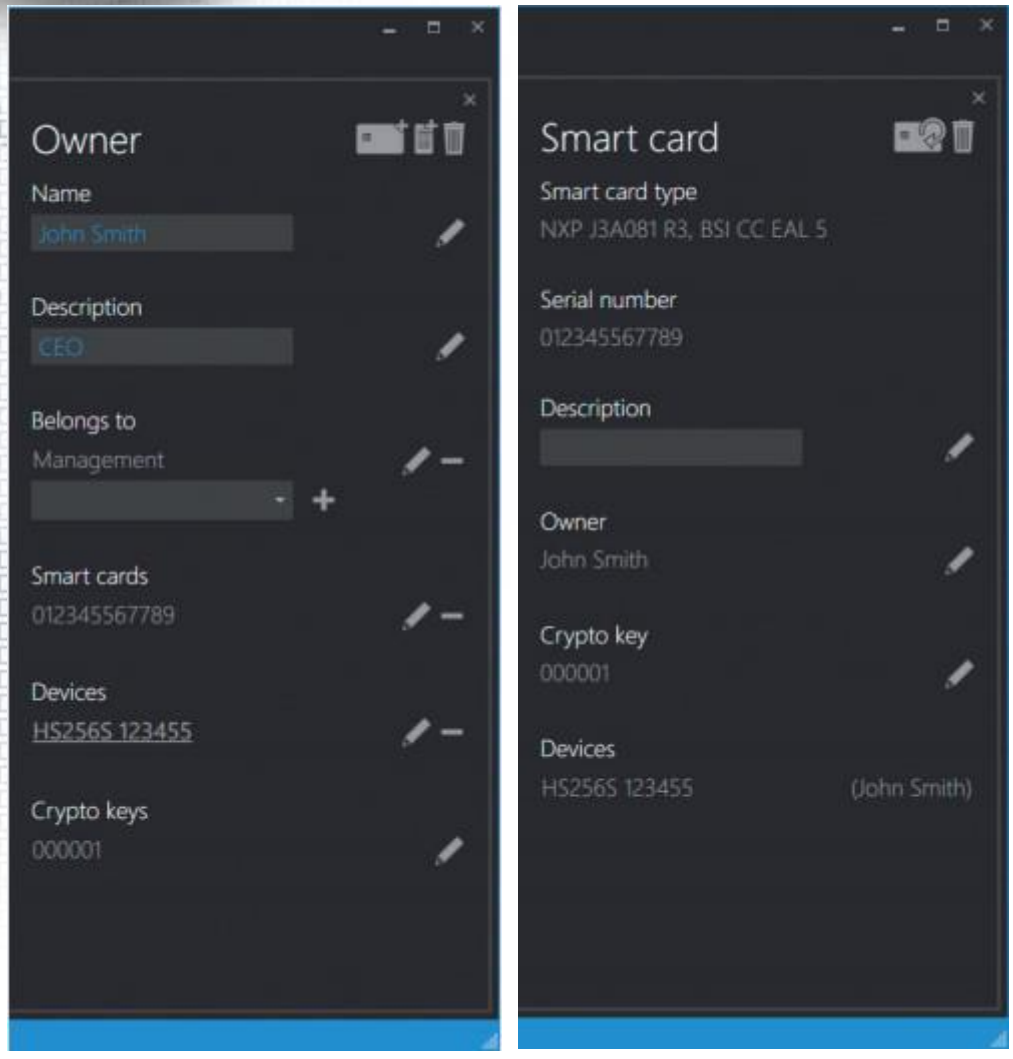

POŠILJATELJ
PAMETNA KARTICA A
PRIJENOS PODATAKA
POŠTA
PRIMATELJ
PAMETNA KARTICA B

SMARTCARD MANAGER 2

- Administracijski softver za sigurnosne diskove visoke sigurnosti, pametne kartice i korisnike
- Centralna administracija svih tvrdih HDD/ SSD diskova
- Registracija svih korisnika, pametnih kartica i diskova u kompaniji



SMARTCARD MANAGER 2



- Ilustracija strukture cijele kompanije
- Pregled svih korištenih diskova, kartica i kriptografskih ključeva
- Puna kontrola pametne kartice na svom računalu
- Sinkronizacija pametne kartice, kreiranje nove, editiranje i brisanje kriptografskih ključeva, promjena PIN-ova

CRYPTO DUAL+ FIPS140 – 2 AES 256

- AES 256 bitna hardverska enkripcija
- Dvostruka lozinka – master lozinka i korisnička lozinka
- Nakon 6 pogrešnog unosa lozinke podaci se automatski brišu
- Nema potrebe za instalacijom softvera
- Nemogućnost pristupa podacima bez ispravne 8-16 lozinke
- FIPS 140-2 level 2

CRYPTO DUAL+ 140 – 2 AES 256

- Automatsko kriptiranje podataka nakon uklanjanja iz računala
- Brojanje pogrešnih unosa se nastavlja
- Mogućnost ostavljanja kontakt podataka na disku bez da se kompromitiraju kodirani podaci
- Plug & Play
- Memorija od 2GB do 128GB

CRYPTO DUAL+ FIPS197 AES256

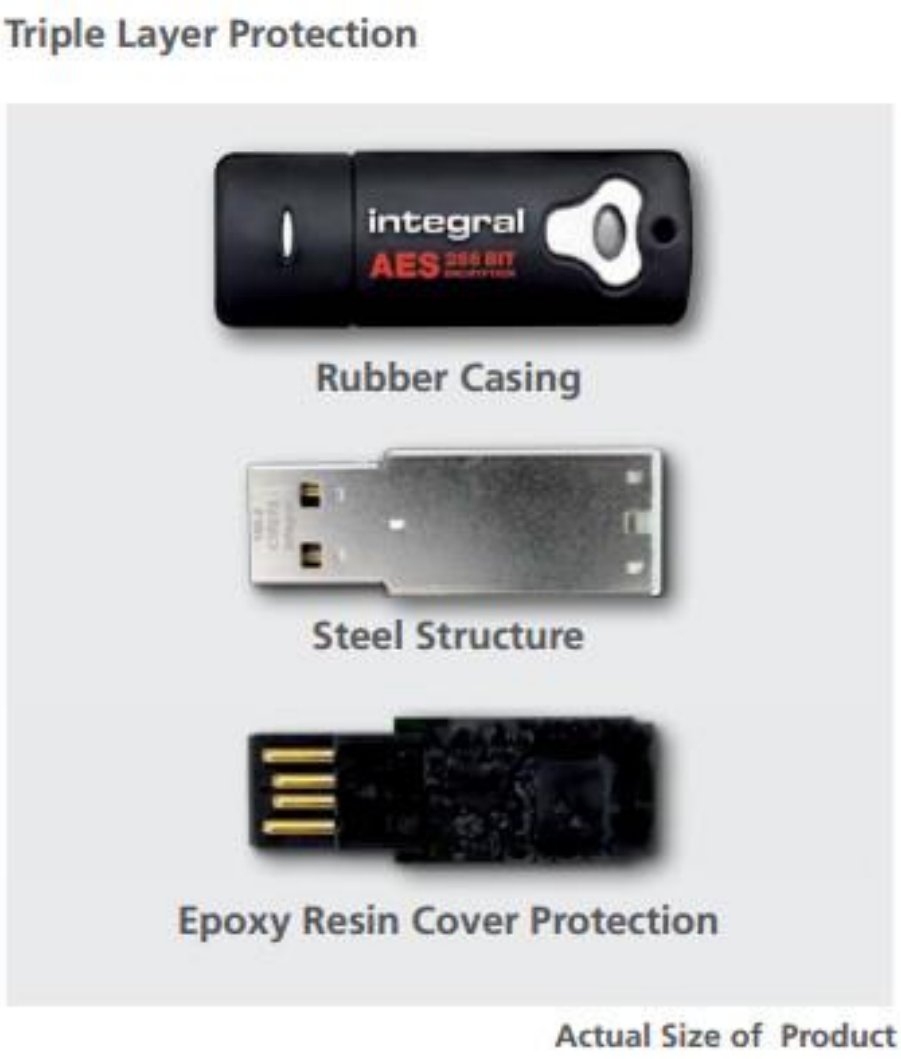
- AES 256 bitna hardverska enkripcija
- Svi podaci spremljeni na USB su zaštićeni
- Dvostruka lozinka – master i user lozinka
- Nema potrebe za dodatnim softverima
- Nemogućnost pristupa podacima bez odgovarajuće 8-16 znakovne lozinke

CRYPTO DUAL+ FIPS197 AES256

- Podaci se automatski brišu nakon 6 neuspješnih pokušaja
- Pamti neuspjele pokušaje
- Mogućnost spremanja kontakt podataka bez da se vide i ugroze zaštićeni podaci
- Svaki USB pin ima na sebi 7 znamenkasti kod te se može vidjeti kojem korisniku pripada
- Od 2GB do 128GB

CRYPTO USB FIPS 140-2 /197

- Primjena - Zaštita podataka, projekata, financija, računovodstva, razvoja i sl. protiv neovlaštenog pristupa
- AES 256 bitna hardverska enkripcija
- FIPS 140 Level 2 ili FIPS 197 ovisno o modelu
- Potrebno postaviti lozinku prije korištenja
- Nema potrebe za dodatnim softverima



CRYPTO USB FIPS 140-2 /197

- Nemogućnost pristupa podacima bez odgovarajuće lozinke
- Automatsko brisanje podataka nakon 6 krivih unosa
- Automatsko zaključavanje nakon isključivanja iz računala
- Brojanje krivih unosa lozinke
- Od 2GB do 32GB

CRYPTO SSD AES 256

- Kriptirani SSD disk
- AES 256 bitna hardverska enkripcija
- FIPS 197 certifikat
- Idealna zamjena za standardni tvrdi disk u računalu ili laptopu
- Dvostruka lozinka – master i user
- Svi podaci na disku kriptirani uključujići OS
- Prije korištenja potrebno podesiti lozinku 8-16 znamenaka

CRYPTO SSD AES 256

- Kriptirani podaci automatski pobrisani kad se 6 puta unese pogrešna lozinka (može se podesiti do 20 pogrešnih unosa)
- Radi neovisno o BIOS-u
- Brzine čitanja i pisanja od 420 MB/s i 340 MB/s
- Nema pomičnih djelova
- Ne zagrijava se
- Tih rad
- Mala potrošnja energije
- Od 64GB do 512GB

U PRIPREMI

- KRIPTIRANJE MOBILNIH TELEFONA