Osogovska 10
11030 Belgrade
Serbia

Phone/Fax: +381 11 30 58 612
E-mail: *office@netsetglobal.rs*

Kriptografski midlver TrustEdge ID

- Opis verzija -

Autor: Mihajlo Cvetanović
Verzija: 1.3
Datum: 30.1.2018

Sadržaj

Istorija promena dokumenta

Datum	Autor	Izmena	Verzija
12. jan. 2016.	A. Radulović	Prva verzija dokumenta	1.0
30. dec. 2016.	M. Cvetanović	Izmene u TrustEdgeID verziji 2.2.2	1.1
30. mar. 2017.	M. Cvetanović	Izmene u TrustEdgeID verziji 2.2.3	1.2
30. jan. 2018.	M. Cvetanović	Izmene u TrustEdgeID verziji 2.2.4	1.3

Uvod

Uloga ovog dokumenta je da opiše izmene koje su sadržane u različitim verzijama Trust Edge ID kriptografskog midlvera.

U ovom dokumentu će biti obuhvaćene izmene počev od verzije midlvera 2.2.0 koja donosi nekoliko značajnih unapređenja, opisanih u nastavku dokumenta.

Prilikom navođenja izmena koje donose pojedine verzije midlvera, same izmene će biti grupisane po komponentama koje ga čine: Smart Card mini drajver, PKCS#11 biblioteka, Instalacija, Alat za upravljanje kriptografskim tokenom – smart karticom (u nastavku teksta Token Manager).

Šta je novo u Trust Edge ID 2.2.0

Ova verzija midlvera sadrži izmene sledećih komponenata:

Instalacija:

- Instalira sve programske artifakte na predefinisanu putanju „C:/Program Files/TrustEdgeId“ (Netset nije naveden u putanji),
- Deinstalira sve prethodne instalacije Trust Edge midlvera. Prethodne instalacije obuhvataju kriptografski midlver za novu verziju lične karte, službene legitimacije Vojske Srbije, kartice koje izdaje Privredna komora Srbije, nove zdravstvene kartice koje izdaje RFZO. Najnovija verzija instalacije će deinstalirati bilo koji od navedenih midlvera i podržati sve nabrojane smart kartice.
- Registruje samo one kartice koje zaista treba da budu registrovane, uz jasnu konvenciju imenovanja. Kada se završi instalacija, na datom računaru će biti registrovani sledeći parovi naziv, vrednost ATR:
    - Gemalto Multiapp 80K with NetSeT PKI, 3B FF 94 00 00 81 31 80 43 80 31 80 65 B0 85 02 01 F3 12 0F FF 82 90 00 79
    - NXP JCOP v2.4.1 80K with NetSeT PKI, 3B F8 13 00 00 81 31 FE 45 4A 43 4F 50 76 32 34 31 B7
    - NXP JCOP21 v2.3.1 with NetSeT PKI, 3B FA 13 00 00 81 31 FE 45 4A 43 4F 50 32 31 56 32 33 31 91
    - NXP JCOP21 v2.4.1 with NetSeT PKI, 3B F4 13 00 00 81 31 FE 45 52 46 5A 4F ED.

PKCS#11 biblioteka:

- Podržano je nekoliko dodatnih kriptografskih algoritama i unapređena je interoperabilnost rešenja.

Smart Card mini drajver: neznatne izmene.

Šta je novo u Trust Edge ID 2.2.1

Ova verzija midlvera sadrži izmene sledećih komponenata:

Token Manager:

- Interne verzije programskih modula (smart card mini drajver, pkcs#11 biblioteka, Token Manager) se prikazuju u Report kartici,
- Uklonjena mogućnost za brisanje i formatiranje kartice.

Šta je novo u Trust Edge ID 2.2.2

Ova verzija midlvera sadrži izmene sledećih komponenata:

Token Manager:

- Omogućeno brisanje sertifikata iz magacina sertifikata kada se kartica izvadi iz čitača. Funkcionalnost se može isključiti u novoj kartici *Configuration*.
- Uvedeno upozorenje korisniku ako je neki od sertifikata na kartici pred istekom (15 ili manje dana do isticanja), ili ako je vremeneski nevažeći (datum na kompjuteru ne ulazi u opseg datuma za koje sertifikat važi). Upozorenje je u obliku pop-up balona u donjem desnom uglu ekrana (uz sistemsku traku poslova, eng. *system notification area*). Funkcionalnost se može isključiti u novoj kartici *Configuration*.
- Token Manager više ne krahira kada se izvuče kartica.
- Informacija o verzijama modula je pomerena na dno izveštaja u kartici *Report*.

PKCS#11 biblioteka:

- Prilikom gašenja aplikacije u kojoj je učitana biblioteka neće se desiti da aplikacija ostane zaglavljena u spisku aktivnih procesa.
- Sadržaj CKO_DATA objekata se ne učitava prilikom enumeracije objekata na kartici (u C_FindObjectsInit), nego kada se zaista traži sadržaj konkretnog objekta (u C_GetAttributeValue). Tako se brže započinje rad s karticom, ali je efekat uočljiviji sa povećanjem količine bajtova u CKO_DATA objektima.
- Ispravljene manje greške otkrivene tokom opsežnijeg testiranja.

Smart Card mini drajver:

- Biblioteka više ne krahira u nekim situacijama.

Šta je novo u Trust Edge ID 2.2.3

Ova verzija midlvera sadrži izmene sledećih komponenata:

Instalacija:

- Dodata nova smart kartica:
  - Gemalto Multiapp 80K IDCore10 with NetSeT PKI, 3B 7A 96 00 00 80 65 A2 01 01 02 3D 72 D6 43
- Posle završene instalacije Token Manager se pokreće automatski.

Token Manager:

- Kada se kartica ubaci u čitač Token Manager može da detektuje neispravnu registraciju smart kartice. Smart kartica je neispravno registrovana ako postoji više od jedne registracije koja se odnosi na datu smart karticu. Detekcija nije ograničena samo na kartice sa kojima TrustEdgeID radi. Ako TrustEdgeID treba da radi sa ubačenom karticom onda treba reinstalirati TrustEdgeID, ili samo popraviti instalaciju (repair)

Šta je novo u Trust Edge ID 2.2.4

Ova verzija midlvera sadrži izmene sledećih komponenata:

Instalacija:

- Uvedena imena tipova dokumenata. Tip dokumenta se detektuje na osnovu podatka u sertifikatu, URL-a ka sertifikatu izdavača (potpisnika sertifikata na smart kartici). Podaci se upisuju u registar na lokaciji HKEY_LOCAL_MACHINE\Software\TrustEdgeID\DocumentTypes. Tipovi dokumenata zamenjuju u kartici Objects tip smart kartice (utvrđeno na osnovu ATR-a kartice) ako je tip dokumenta uspešno određen. Tipovi dokumenata i URL-ovi na osnovu kojih se određuju su sledeći:

Tip dokumenta	URL
Lična karta Republike Srbije	ca.mup.gov.rs/MUPCAGradjani
Korporativna PKS kartica	ca.pks.rs/v2/certs/PKSCAClass1
Kartica zdravstvenog osiguranja	ca.rfzo.rs/cert/RFZOCAOsiguranici

Sve komponente:

- Brisanje objekata sa kartice se kontroliše opcijom u Token Manageru. Ako je opcija uključena onda će i PKCS#11 biblioteka i smart card mini drajver po komandi obrisati ono što se od njih traži. Ako je opcija isključena onda funkcije PKCS#11 biblioteke vraćaju grešku CKR_TOKEN_WRITE_PROTECTED, a funkcije smart card mini drajvera vraćaju grešku SCARD_E_NO_ACCESS. Isključena opcija je podrazumevana vrednost (*default*). Objekti koji se kontrolišu ovom opcijom su sertifikati, kontejneri, kao i elementarni fajlovi i direktorijumi na smart kartici. Opcija je upisana u registru na lokaciji HKEY_CURRENT_USER\Software\TrustEdgeID, u polju AllowSmartCardObjectsDeletion.

Token Manager:

- Upozorenje o isteku sertifikata se daje 30 dana pre isticanja, umesto 15 dana kao do sad.
- Fajl izveštaja (koji se dobija klikom na dugme u Report kartici) je sad u UTF-8 formatu, pa će se videti srpska slova umesto dosadašnjih znakova pitanja.
- Verzija Token Managera je od sad ista kao i verzija celog paketa, u ovom slučaju 2.2.4.

Obe biblioteke:

- Biblioteke više ne krahiraju u nekim situacijama.
- Ispravljeno potencijalno curenje memorije prilikom čitanja sertifikata.