РЕПУБЛИКА СРБИЈА
МИНИСТАРСТВО УНУТРАШЊИХ ПОСЛОВА
Сектор за аналитику, телекомуникационе и информационе технологије
Одељење за информациону безбедност
Одсек за сертификациони систем

Опис функција за Челик апи v1.3

Јануар 2020.

Садржај

Увод

О АПИ-ју

ЧЕЛИК (Читач Електронске ЛИчне Карте) апи служи за очитавање чипа електронске личне карте са оперативним системом Apollo v.2.43 у случају старе личне карте и оперативним системом Gemalto MultiApp у случају нове личне карте. Челик апи се састоји од три фајла (CelikApi.dll, CelikApi.h, и CelikApi.lib) и пратеће документације (овог документа).

ЧЕЛИК апи намењен је превасходно програмерским кућама за интеграцију у пословним системима.

Софтвер и хардвер

За коришћење ЧЕЛИК апија захтева се:

Microsoft Windows оперативни систем

Подржани оперативни систем Windows: Windows XP SP-3, Windows Vista SP-1, Windows 7 SP-1, и Windows 10.

Инсталиран читач смарт картица (по упутству произвођача).

Ради са свим читачима смарт картица који се могу комерцијално набавити код продаваца рачунарске опреме.

Списак функција Челик апија и опис њихових фунционалности

Функције библиотеке Челик апи су следеће:

`EidSetOption`	Контрола рада библиотеке.
`EidStartup`	Иницијализација рада библиотеке, позива се једном на почетку рада
`EidCleanup`	Крај рада са библиотеком, позива се једном на крају рада
`EidBeginRead`	Почетак рада са једном личном картом
`EidEndRead`	Крај рада са личном картом
`EidReadDocumentData`	Читање блока података о документу
`EidReadFixedPersonalData`	Читање блока непроменљивих података
`EidReadVariablePersonalData`	Читање блока променљивих података
`EidReadPortrait`	Читање слике портрета
`EidReadCertificate`	Читање сертификата са картице
`EidChangePassword`	Промена лозинке
`EidVerifySignature`	Верификација блокова података

Да би се користио Челик апи пре било које друге функције треба позвати `EidStartup`, и то само једном. Крај рада са библиотеком се означава позивом функције `EidCleanup`. После извршења функције `EidCleanup`, могуће је поново позвати `EidStartup`.

Сесија са личном картом се отвара позивом функције `EidBeginRead`. Ова функција је неопходна не само за читање података, него и за промену лозинке и верификацију потписа података. Сесија са личном картом се затвара позивом функције `EidEndRead`. Да би се започео рад са новом личном картом неопходно је прво завршити рад са претходном.

Ако се више од једне личне карте чита под истом сесијом подаци неће бити исправни, и може доћи до грешака у читању и верификацији. Стари програми који су читали податке под истом сесијом морају да буду исправљени тако да личним картама приступају у одвојеном сесијама. Привремено решење, без много измена у коду, је укључивање опције `EID_O_KEEP_CARD_CLOSED` функцијом `EidSetOption`. Стари програм ће радити као и раније, али ће приступ картици бити спорији.

У наставку је дат опис свих функција.

EidSetOption

Прототип функције

```
int WINAPI EidSetOption(int nOptionID, UINT_PTR nOptionValue);
```

Улазни аргументи

- Аргумент `nOptionID` типа `int` који представља идентификатор опције. Вредност за овај параметар може бити следећа:

`EID_O_KEEP_CARD_CLOSED`	Контекст са картицом се брише после сваке појединачне операције над картицом

- Аргумент `nOptionValue` типа `int` чије значење зависи од вредности аргумента `nOptionID`. Валидне вредности су следеће:

`EID_O_KEEP_CARD_CLOSED`	0 – опција је искључена 1 – опција је укључена

Излазни аргументи

Нема

Повратна вредност

Функција враћа `EID_OK` ако је успешно извршена или код грешке који је описан у CelikApi.h.

Начин употребе

Функција поставља опцију која контролише рад библиотеке.

Ако је опција `EID_O_KEEP_CARD_CLOSED` укључена онда ће се свака операција над картицом извршавати у посебном контексту. Ова опција је корисна само за стару верзију личне карте (*Apollo*), а игнорише се у раду са новом верзијом (*Java*). Ова опција је предвиђена као привремено решење за кориснике библиотеке који су у ранијој верзији библиотеке (пре 1.1) функцију `EidBeginRead` позивали само једном за све картице, на почетку рада, уместо сваки пут кад се приступа новој картици. Такав код за нову верзију библиотеке треба да се исправи, али ће постојећи код радити (успорено) и ако се укључи наведена опција.

EidStartup

Прототип функције

```
EID_API int WINAPI EidStartup(int nApiVersion);
```

Улазни аргументи

- Аргумент `nApiVersion` типа `int` који представља верзију апија чије се функције позивају. Једина тренутно исправна вредност је 3.

Излазни аргументи

Нема

Повратна вредност

Функција враћа `EID_OK` ако је успешно извршена или код грешке који је описан у CelikApi.h.

Начин употребе

Ова функција се позива само једном (обавезно) на почетку рада са апијем. На крају рада се обавезно мора позвати `EidCleanup`.

EidCleanup

Прототип функције

```
EID_API int WINAPI EidCleanup();
```

Улазни аргументи

Нема

Излазни аргументи

Нема

Повратна вредност

Функција враћа `EID_OK` ако је успешно извршена или код грешке који је описан у CelikApi.h.

Начин употребе

Ова функција се позива само једном (обавезно) на крају рада са апијем.

EidBeginRead

Прототип функције

```
EID_API int WINAPI EidBeginRead(LPCSTR szReader, int* pnCardType);
```

Улазни аргументи

- Аргумент `szReader` типа `LPCSTR` је име смарт кард читача који се користи.

Излазни аргументи

- Аргумент `pnCardType` типа показивача на `int` је излазни параметар, којим корисник може да установи који је тип личне карте. Вредности које функкција може да врати су следеће:

`EID_CARD_ID2008 = 1`	Стара лична карта, Apollo
`EID_CARD_ID2014 = 2`	Нова лична карта, Gemalto
`EID_CARD_IF2020 = 3`	Лична карта за странце

  Овај параметар може имати вредност 0 (односно NULL) и у том случају функција га игнорише. Игнорисање се ипак не препоручује кад се читају подаци.

Повратна вредност

Функција враћа `EID_OK` ако је успешно извршена или код грешке који је описан у CelikApi.h.

Начин употребе

Ова функција се позива обавезно пре позива блока команди за читање података и сертификата са личне карте, као и за промену лозинке и верификацију потписа података. На крају блока се обавезно мора позвати `EidEndRead`.

Пре позива ове функције мора се успешно извршити позив функције `EidStartup`.

EidEndRead

Прототип функције

```
EID_API int WINAPI EidEndRead();
```

Улазни аргументи

Нема

Излазни аргументи

Нема

Повратна вредност

Функција враћа `EID_OK` ако је успешно извршена или код грешке који је описан у CelikApi.h.

Начин употребе

Ова функција се позива обавезно на крају блока команди за приступ личној карти.

EidReadDocumentData

Прототип функције

```
int WINAPI EidReadDocumentData(PEID_DOCUMENT_DATA pData);
```

Улазни аргументи

Нема

Излазни аргументи

- Аргумент `pData` је типа `PEID_DOCUMENT_DATA` који представља показивач на структуру у коју се смештају подаци о документу са личне карте. Структура мора бити унапред алоцирана. Поменута структура је декларисана у CelikApi.h.

Повратна вредност

Функција враћа `EID_OK` ако је успешно извршена или код грешке који је описан у CelikApi.h.

Начин употребе

Функција чита податке везане за сам документ и смешта их у излазну структуру на коју показује аргумент `pData`.

Подаци су у UTF-8 формату и не завршавају се NUL карактером.

Пре позива ове функције мора се успешно извршити позив функције `EidBeginRead`.

Поља `documentSerialNumber` и `chipSerialNumber` су валидна само за личну карту за странце (`EID_CARD_IF2020`).

EidReadFixedPersonalData

Прототип функције

```
int WINAPI EidReadFixedPersonalData(PEID_FIXED_PERSONAL_DATA pData);
```

Улазни аргументи

Нема

Излазни аргументи

- Аргумент `pData` је типа `PEID_FIXED_PERSONAL_DATA` који представља показивач на структуру у коју се смештају непроменљиви лични подаци са личне карте. Структура мора бити унапред алоцирана. Поменута структура је декларисана у CelikApi.h.

Повратна вредност

Функција враћа `EID_OK` ако је успешно извршена или код грешке који је описан у CelikApi.h.

Начин употребе

Функција чита непроменљиве личне податке из личне карте и смешта их у излазну структуру на коју показује аргумент `pData`.

Подаци су у UTF-8 формату и не завршавају се NUL карактером.

Пре позива ове функције мора се успешно извршити позив функције `EidBeginRead`.

Поља `statusOfForeigner` и `nationalityFull` су валидна само за личну карту за странце (`EID_CARD_IF2020`).

EidReadVariablePersonalData

Прототип функције

```
int WINAPI EidReadVariablePersonalData(
      PEID_VARIABLE_PERSONAL_DATA pData);
```

Улазни аргументи

Нема

Излазни аргументи

- Аргумент `pData` је типа `PEID_VARIABLE_PERSONAL_DATA` који представља показивач на структуру у коју се смештају променљиви подаци са личне карте. Структура мора бити унапред алоцирана. Поменута структура је декларисана у CelikApi.h.

Повратна вредност

Функција враћа `EID_OK` ако је успешно извршена или код грешке који је описан у CelikApi.h.

Начин употребе

Функција чита променљиве податке из личне карте и смешта их у излазну структуру на коју показује аргумент `pData`.

Подаци су у UTF-8 формату и не завршавају се NUL карактером.

Пре позива ове функције мора се успешно извршити позив функције `EidBeginRead`.

EidReadPortrait

Прототип функције

```
int WINAPI EidReadPortrait(PEID_PORTRAIT pData);
```

Улазни аргументи

Нема

Излазни аргументи

- Аргумент `pData` је типа `PEID_PORTRAIT` који представља показивач на структуру у коју се смешта слика са личне карте. Структура мора бити унапред алоцирана. Поменута структура је декларисана у CelikApi.h.

Повратна вредност

Функција враћа `EID_OK` ако је успешно извршена или код грешке који је описан у CelikApi.h.

Начин употребе

Функција чита слику из личне карте и смешта је у излазну структуру на коју показује аргумент `pData`.

Слика је у JPG формату.

Пре позива ове функције мора се успешно извршити позив функције `EidBeginRead`.

EidReadCertificate

Прототип функције

```
int WINAPI EidReadCertificate(
      PEID_CERTIFICATE pData, int certificateType);
```

Улазни аргументи

- Аргумент `certificateType` типа `int` који представља тражени тип сертификата. Вредности за овај параметар могу бити следеће:

`EID_Cert_MoiIntermediateCA`	Сертификат потписника друга два сертификата
`EID_Cert_User1`	Сертификат власника за аутентикацију
`EID_Cert_User2`	Сертификат власника за потписивање

Излазни аргументи

Аргумент `pData` је типа `PEID_CERTIFICATE` који представља показивач на структуру у коју се смешта сертификат са личне карте. Структура мора бити унапред алоцирана. Поменута структура је декларисана у CelikApi.h.

Повратна вредност

Функција враћа `EID_OK` ако је успешно извршена или код грешке који је описан у CelikApi.h.

Начин употребе

Ова функција се може користити само за стари тип личне карте (Apollo). За нове личне карте функција враћа повратну вредност `EID_E_UNABLE_TO_EXECUTE`. Челик апи нема функционалност читања сертификата са нове личне карте.

Функција чита податке везане за сам документ и смешта их у излазну структуру на коју показује аргумент `pData`.

Сертификат је у X.509 формату.

Пре позива ове функције мора се успешно извршити позив функције `EidBeginRead`.

EidChangePassword

Прототип функције

```
EID_API int WINAPI EidChangePassword(
      LPCSTR szOldPassword, LPCSTR szNewPassword, int* pnTriesLeft);
```

Улазни аргументи

- Аргумент `szOldPassword` типа `LPCSTR` који је тренутна лозинка корисника.
- Аргумент `szNewPassword` типа `LPCSTR` који је нова лозинка корисника.

Излазни аргументи

- Аргумент `pnTriesLeft` типа показивача на `int` који је број преосталих покушаја уноса лозинке, пре него што се смарт картица не заблокира. Овај параметар може имати вредност 0 (односно NULL) и у том случају функција га игнорише.

Повратна вредност

Функција враћа `EID_OK` ако је успешно извршена или код грешке који је описан у CelikApi.h.

Начин употребе

Ова функција се може користити само за стари тип личне карте (Apollo). За нове личне карте функција враћа повратну вредност `EID_E_UNABLE_TO_EXECUTE`. Челик апи нема функционалност промене лозинке на новој личној карти.

Функција мења лозинку корисника на личној карти. Лозинка може да има најмање 5, а највише 16 знакова. Формат за оба параметра је кодна страна ISO-8859-1. Сви симболи у овој кодној страни су у UTF-8 формату представљени једним бајтом по симболу.

Пре позива ове функције мора се успешно извршити позив функције `EidBeginRead`.

EidVerifySignature

Прототип функције

```
int WINAPI EidVerifySignature(UINT nSignatureID);
```

Улазни аргументи

- Аргумент nSignatureID типа unsigned int који представља идентификатор потписа. Вредности за овај параметар могу бити следеће:

EID_SIG_CARD	Потпис кључних података у документу
EID_SIG_FIXED	Потпис блокова непроменљивих података
EID_SIG_VARIABLE	Потпис блока промељивих података
EID_SIG_PORTRAIT	Потпис слике портрета

Излазни аргументи

Нема

Повратна вредност

Функција враћа EID_OK ако је успешно извршена или код грешке који је описан у CelikApi.h.

Начин употребе

Потпис слике портрета постоји само у старом типу личне карте (Apollo). У новој личној карти (Gemalto) потпис блокова непроменљивих података покрива и портрет. Ако се у случају нове личне карте позове ова функција с параметром EID_SIG_PORTRAIT функција враћа повратну вредност EID_E_UNABLE_TO_EXECUTE.

Функција, на основу параметра с којим је позвана, чита из личне карте одговарајуће податке, сертификат потписника тих података, као и сам потпис. Ланац поверења за сертификат потписника се успоставља користећи расположиве сертификате из складишта сертификата (енг. *certificate store*) оперативног система. На крају се проверава да ли потпис података одговара датом сертификату.

Ако функција не може да успостави ланац поверења за сертификат потписника онда ће вратити вредност грешке EID_E_SECFORMAT_CHECK_CERT_ERROR. Овај код не значи да подаци нису исправни, него да верификација није успела због тога што није најпре успостављен ланац поверења.

Пре позива ове функције мора се успешно извршити позив функције EidBeginRead.