



Опис функција за Челик апи v1.4.2

Децембар 2024.

Садржај

Увод	3
О АПИ-ју	3
Софтвер и хардвер.....	3
Функције Челик апија	4
EidSetOption	5
EidStartup	6
EidCleanup.....	7
EidBeginRead	8
EidEndRead	9
EidReadDocumentData	10
EidReadFixedPersonalData	11
EidReadVariablePersonalData	12
EidReadPortrait	13
EidReadCertificate.....	14
EidChangePassword	16
EidVerifySignature.....	17
Структуре Челик апија	18
EID_DOCUMENT_DATA	19
EID_FIXED_PERSONAL_DATA	20
EID_VARIABLE_PERSONAL_DATA	21
EID_PORTRAIT	22
EID_CERTIFICATE	23

Увод

О АПИ-ју

ЧЕЛИК (Читач Електронске Личне Карте) апи служи за читавање чипа електронске личне карте са оперативним системом Apollo v2.43 у случају старе личне карте (издате пре 18.08.2014. године) и оперативним системима Gemalto MultiApp и Veridos SmartCafe у случају нове личне карте (издате после 18.08.2014. године). 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.

Поред личних карата грађана Републике Србије овај апи може да чита и личну карту за странце, као и боравишну дозволу.

Софтвер и хардвер

За коришћење ЧЕЛИК апија захтева се:

Microsoft Windows оперативни систем

Подржани оперативни системи:

- Windows: Windows Vista SP-1, Windows 7 SP-1, Windows 10, Windows 11.

Инсталиран читач паметних картица (по упутству произвођача).

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

Функције Челик апија

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. Веома 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:

<code>EID_O_KEEP_CARD_CLOSED</code>	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:

<code>EID_O_KEEP_CARD_CLOSED</code>	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 (*Gemalto* и *Veridos*). 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 4.

Излазни аргументи

Нема

Повратна вредност

Функција враћа `EID_OK` ако је успешно извршена или код грешке који је описан у `SelikApi.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 читача паметних картица који се користи.

Излазни аргументи

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

<code>EID_CARD_ID2008 = 1</code>	Стара лична карта, Apollo
<code>EID_CARD_ID2014 = 2</code>	Нова лична карта, Gemalto или Veridos
<code>EID_CARD_IF2020 = 3</code>	Лична карта за странце
<code>EID_CARD_RP2024 = 4</code>	Боравишна дозвола 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`.

Поље `documentSerialNumber` је валидно само за личну карту за странце (`EID_CARD_IF2020`) и боравишну дозволу (`EID_CARD_RP2024`). Поље `chipSerialNumber` је валидно само за личну карту за странце. Поље `documentName` је валидно само за боравишну дозволу.

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`.

Поље `nationalityFull` је валидно само за личну карту за странце (`EID_CARD_IF2020`) и боравишну дозволу (`EID_CARD_RP2024`). Поље `statusOfForeigner` је валидно само за личну карту за странце. Поља `purposeOfStay` и `eNote` су валидна само за боравишну дозволу.

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
EID_Cert_SIG_FIXED	Сертификат потписника блока непроменљивих података
EID_Cert_SIG_VARIABLE	Сертификат потписника блока променљивих података

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

За параметар `certificateType` вредности `EID_Cert_MoiIntermediateCA`, `EID_Cert_User1`, и `EID_Cert_User2` се могу користити само за стари тип личне карте (Apollo). Од верзије Челик АПИ 1.4.2. вредности `EID_Cert_SIG_FIXED` и `EID_Cert_SIG_VARIABLE` се могу користити само за нове личне карте. Пошто интерфејс није мењан, него су само додати нови типови сертификата, овом приликом није промењена верзија апија, која се наводи у функцији `EidStartup`.

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

Сертификат је у X.509 формату.

Потписник података може бити радник МУП. У сертификату радника МУП се налазе лични подаци власника. Ти подаци подлежу закону о заштити података о личности. Челик апликација на пример приликом приказа власника сертификата замењује ЈМБГ власника звездицама.

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 паметна картица блокира. Овај параметар може да има 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 променљивих 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 и Veridos) 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`.

Структуре Челик апија

Структуре челик апија одговарају блоковима података на картици. Структуре су следеће:

EID_DOCUMENT_DATA	Подаци о самом документу
EID_FIXED_PERSONAL_DATA	Непроменљиви подаци власника
EID_VARIABLE_PERSONAL_DATA	Променљиви подаци власника
EID_PORTRAIT	Портрет власника
EID_CERTIFICATE	Сертификат

Структуре су исте за све типове докумената, али сва поља у њима нису намењена за сваки тип документа.

Структуре су се мењале са верзијама апија. Нова поља су додавана, или постојећа поља проширивана. Верзија апија се бира параметром `nApiVersion` приликом позива функције `EidStartup`. Када се у коду промени верзија потребно је прилагодити код. У најмању руку потребно је поново компајлирати код, да би се користиле нове верзије структуре.

За пројекте који нису реализовани у програмским језицима C и C++, и који не могу да директно референцирају фајл заглавља `CelikApi.h`, потребно је да се посебно обрати пажња на садржај и дужину свих поља у свим структурама, приликом прилагођавања пројекта новој верзији апија.

Сваки податак у свакој структури има два поља, бафер за садржај и дужину податка у том баферу, у бајтовима. Величина бафера, а тиме и максимална дужина податка је дата константом, која је такође дефинисана у фајлу заглавља. На пример, име власника картице (енг. *given name*) има два поља у структури `EID_FIXED_PERSONAL_DATA`, са величином бафера дефинисаном константом:

```
const int EID_MAX_GivenName = 200;

typedef struct
{
    ...
    char givenName[EID_MAX_GivenName];
    int givenNameSize;
    ...
} EID_FIXED_PERSONAL_DATA;
```

Програмери могу да претпоставе да су сва поља енкодирана у UTF-8, мада нека поља могу да имају знаке само из ASCII подскупа.

У наставку су детаљније описане све структуре, као и која поља су релевантна за сваки тип документа.

EID_DOCUMENT_DATA

Опис

Структура садржи податке о документу, на пример датум до ког документ важи. Ови подаци се не могу променити на картици.

Подаци у структури

У следећој табели дати су подаци у овој структури, са кратким описом и ознаком да се податак користи за сваки од четири типова докумената које апи подржава. Двоцифрени број после типа означава годину у којој је тип уведен.

Име податка	Опис	ID08	ID14	IF20	RP24
Doc Reg No	Регистарски број документа	✓	✓	✓	✓
Document Type	Тип документа		✓	✓	✓
Issuing Date	Датум издавања	✓	✓	✓	✓
Expiry Date	Датум важења	✓	✓	✓	✓
Issuing Authority	Ауторитет који је издао документ	✓	✓	✓	✓
Document Serial Number	Серијски број документа			✓	✓
Chip Serial Number	Серијски број чипа картице			✓	
Document Name	Име документа				✓

Тип документа је двословна ознака, уведена тек од нове ID картице. Зато и није дефинисан за оригинални ID документ. Ако се у будућности деси да буде уведена нова верзија неког документа, као што се то десило са ID документом у 2014. години, ова ознака се неће променити за тај документ. Табела вредности за тренутне типове докумената је следећа:

EID_CARD_ID2008	EID_CARD_ID2014	EID_CARD_IF2020	EID_CARD_RP2024
	ID	IF	RP

Последње промене

У верзији 4 апија, са увођењем типа документа RP, у овој структури промењено је следеће:

- Додата су поља за Document Name.

EID_FIXED_PERSONAL_DATA

Опис

Структура садржи непроменљиве податке о власнику, на пример име власника. Ови подаци се не могу променити на картици.

Подаци у структури

У следећој табели дати су подаци у овој структури, са кратким описом и ознаком да се податак користи за сваки од четири типова докумената које апи подржава. Двоцифрени број после типа означава годину у којој је тип уведен.

Име податка	Опис	ID08	ID14	IF20	RP24
Personal Number	Јединствени матични број	✓	✓	✓	✓
Surname	Презиме	✓	✓	✓	✓
Given Name	Име	✓	✓	✓	✓
Parent Given Name	Име родитеља	✓	✓		
Sex	Пол	✓	✓	✓	✓
Place Of Birth	Место рођења	✓	✓		
State Of Birth	Држава рођења	✓	✓	✓	✓
Date Of Birth	Датум рођења	✓	✓	✓	✓
Community of Birth	Општина рођења	✓	✓		
Status Of Foreigner	Статус странца			✓	
Nationality	Националност			✓	✓
Purpose Of Stay	Сврха боравка странца				✓
E-Note	Напомена о боравку странца				✓

Последње промене

У верзији 4 апија, са увођењем типа документа RP, у овој структури промењено је следеће:

- Додата су поља за Purpose Of Stay.
- Додата су поља за E-Note.

EID_VARIABLE_PERSONAL_DATA

Опис

Структура садржи променљиве податке о власнику, углавном везане за адресу становања. Ови подаци се могу променити.

Подаци у структури

У следећој табели дати су подаци у овој структури, са кратким описом и ознаком да се податак користи за сваки од четири типова докумената које апи подржава. Двоцифрени број после типа означава годину у којој је тип уведен.

Име податка	Опис	ID08	ID14	IF20	RP24
State	Држава становања	✓	✓	✓	
Community	Општина	✓	✓	✓	✓
Place	Место	✓	✓	✓	✓
Street	Улица	✓	✓	✓	✓
House Number	Кућни број	✓	✓	✓	✓
House Letter	Кућно слово	✓	✓	✓	✓
Entrance	Улаз	✓	✓	✓	✓
Floor	Спрат	✓	✓	✓	✓
Apartment Number	Број стана	✓	✓	✓	✓
Address Date	Датум промене адресе		✓	✓	✓
Adress Label	Врста адресе		✓	✓	

Последње промене

У верзији 4 апија нема промена у овој структури.

EID_PORTRAIT

Опис

Структура садржи портрет власника, у JPEG формату. Овај податак се не може променити.

Подаци у структури

У следећој табели дати су подаци у овој структури, са кратким описом и ознаком да се податак користи за сваки од четири типова докумената које апи подржава. Двоцифрени број после типа означава годину у којој је тип уведен.

Име податка	Опис	ID08	ID14	IF20	RP24
Portrait	Портрет власника	✓	✓	✓	✓

Последње промене

У верзији 4 апија нема промена у овој структури.

EID_CERTIFICATE

Опис

Структура садржи сертификат власника, у X.509 DER формату. Овај податак се не може променити.

Подаци у структури

У следећој табели дати су подаци у овој структури, са кратким описом и ознаком да се податак користи за сваки од четири типова докумената које апи подржава. Двоцифрени број после типа означава годину у којој је тип уведен.

Име податка	Опис	ID08	ID14	IF20	RP24
Certificate	Сертификат власника	✓	✓	✓	✓

Последње промене

У верзији 4 апија нема промена у овој структури.