CryptoMate EVO

User Manual • Uživatelský manuál • Užívateľský manuál • Használati utasítás • Benutzerhandbuch

Dear customer,

Thank you for purchasing our product. Please read the following instructions carefully before first use and keep this user manual for future reference. Pay particular attention to the safety instructions. If you have any questions or comments about the device, please contact the customer line.

✉ www.alza.co.uk/kontakt

✆ +44 (0)203 514 4411

Importer Alza.cz a.s., Jankovcova 1522/53, Holešovice, 170 00 Prague 7, www.alza.cz

Introduction

The CryptoMate EVO contains an ACOS5-EVO cryptographic smart card module. The ACOS5-EVO cryptographic smart card module offers advanced asymmetric and symmetric cryptographic algorithms such as ECC and RSA and is compliant with international standards for PKI smart cards such as FIPS 14-2 (US Federal Information Processing Standards) Level 3 and CC EAL 5+ (chip level).

The CryptoMate EVO is similar in appearance to the CryptoMate Nano, but it can be easily distinguished when plugged in the PC with its Green LED. PC applications will recognize it through its PCSC and Driver Name: ACS CryptoMate EVO. It also offers higher memory and more advanced cryptographic functionalities compared to the CryptoMate Nano.

Features

Cryptographic Smart Card Features

The CryptoMate EVO contains the ACOS5-EVO cryptographic smart card module, which has the following features:

Communication Protocols

- T=0, T=1 with baud up to 446,400 bps

Memory

- Capacity: 192Kb
- EEPROM Endurance: 500,000 erase/write cycles
- Data Retention: 30 years

Cryptographic Capabilities

The ACOS5-EVO supports a number of cryptographic algorithms, including:

- ECC: Curves P-224/P-256/P-384/P-521
- RSA: 512 – 4096 bits in 256 bits increments
- AES: 128/192/256-bits (ECB, CBC)
- DES/3DES: 56/112/168-bits (ECB, CBC)
- Hash: SHA1, SHA224, SHA256, SHA384, SHA512
- MAC: CBC-MAC (DES/3DES, AES), CMAC (3DES, AES)

Random Number Generation

- Deterministic RNG according to FIPS 140-2
- Non-deterministic RNG compliant to AIS-31

File Security

- Private and secret key file read access can be set to “Never”
- File access condition capability with ISO 7816-compliant Secure Attribute-Compact. File access is only allowed if the proper security conditions are met (e.g., PIN submissions)
- Command execution condition capability per Dedicated File (DF) with ISO 7816-compliant Secure Attribute-Extended. Commands are allowed only if the proper security conditions are met (e.g., PIN submission)
- Secure Messaging function for confidential and authenticated data transfer
- Mutual authentication (terminal-co-card and card-to-terminal) with session key generation for encryption and MAC
- Anti-tearing Function Support

Compliance to Standards

- Compliance with ISO 7816 Parts 1,2.3,4, 8, and 9
- Compliance with FIPS 140-2 Level 3
- Certified with Common Criteria ELA 5+ (Chip Level)

Token Features

Physical Characteristics

- Green Status LED
- Lightweight: 4.61 g
- Extremely small: 29.25 mm x 14.80 mm x 10.28 mm
- Keychain hole
- Tamper-evident casing
- Smart card power supply through USB port

Compliance to Standards

- USB Full Speed Interface
- CCID-compliant (Plug and Play)
- CE and FCC-certified
- RoHS-compliant
- REACH-certified
- Microsoft WHQL-certified
- Supports Android 3.1 and later

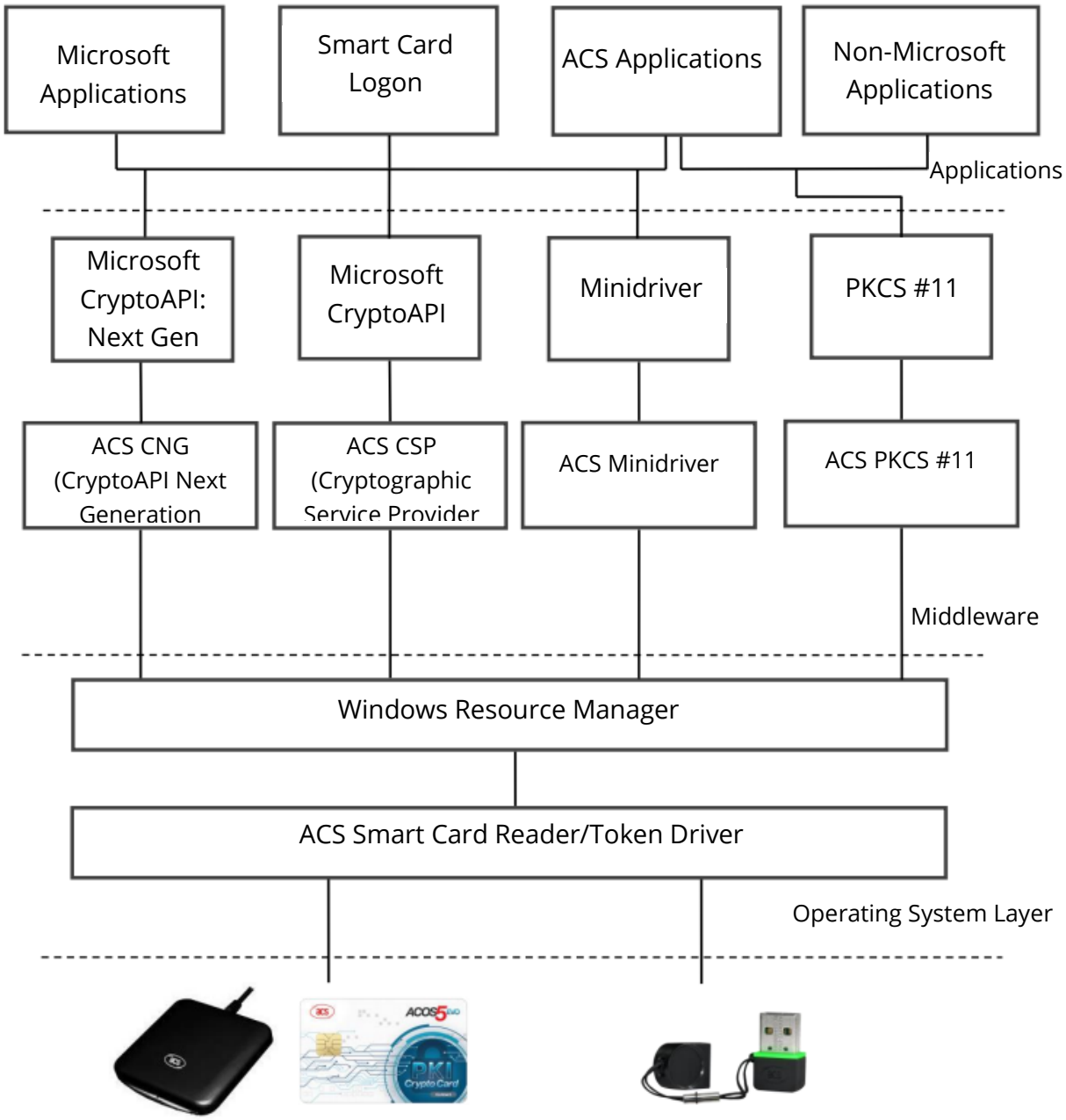
Typical Applications

- e-Government
- e-Healthcare
- Banking and Payment
- Network Security
- Access Control
- Public Key Infrastructure
- Digital Signature

Middleware

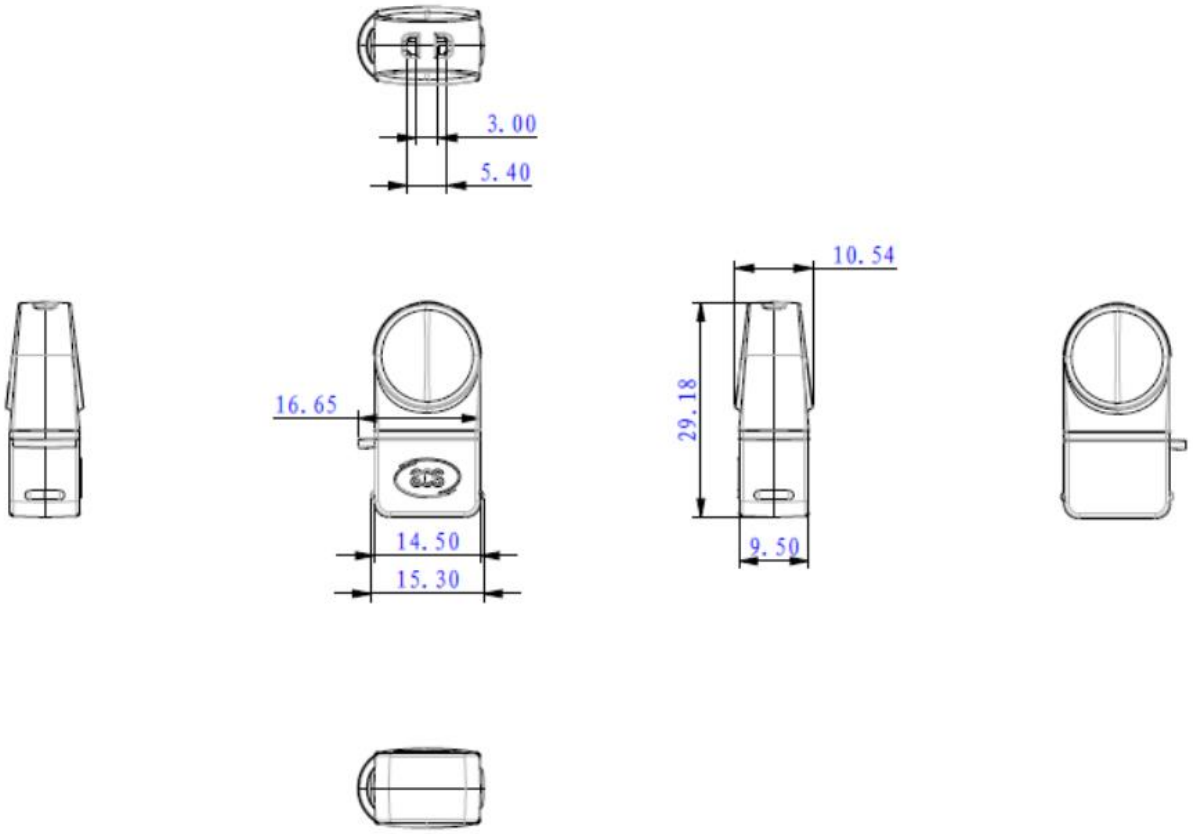
To use CryptoMate EVO for PKI applications with digital certificates, an applicable middleware id needed.

ACS offers software solutions such as the ACOS5 Minidriver and ACOS5-EVO PKI Kit so that the ACOS5-EVO and the CryptoMate EVO can be used with other third-party applications as shown in the figure below:



Please contact us at info@acs.com.hk for inquiries about the middleware supports for the CryptoMate EVO token.

Technical Specifications



Physical Characteristics

Dimensions	29.18 mm (L) x 14.50 mm (W) x 10.54 mm (H)
Weight	4.61 g
Color	Black

ACOS5-EVO Cryptographic Smart Card Module

Memory Size	192 KB
Endurance	500,000 write/erase cycles
Data Retention	30 years
Cryptographic Capability	ECC: Curves P-224/P-256/P-384/P-521 RSA: 512 – 4096 bits in 256 bits increments AES: 128/192/256-bits (ECB, CBC) DES/3DES: 56/112/168-bits (ECB, CBC) MAC: CBC-MAC (DES/3DES, AES) CMAC (3DES, AES)
Hashing Capabality	SHA1, SHA 224, SHA256, SHA384, SHA512

USB Host Interface

Protocol	USB CCID
Connector Type	Standard Type A
Power Source	From USB port
Speed	USB Full Speed (12 Mbps)

Built-in Peripherals

LED	Green
Casing	Tamper-evident
Others	Keychan hole for portability

Operating Conditions

Temperature	0°C - 50°C
Humidity	Max. 90% (non-condensing)
MTBF	500,000 hrs

Certifications/Compliance

ISO 7816, USB Full Speed, Common Criteria ELA5+ (Chip Level), PC/SC, CCID, CE, FCC, RoHS, REACH, FIPS, 140-2 Level 3 (USA), Microsoft WHQL

Middleware Support

ACS PKCS #11, ACS CSP (based on Microsoft's CryptoAPI), ACS CNG (based on Microsoft's CNG)
ACS Minidriver
X.509 v3 Certificate Storage (can store more than 10 Key Pairs)

Device Driver Operating System Support

Windows 7, Windows 8, Windows 8.1, Windows 10
Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016
Linux, Mac OSM Android 3.1 and later

Warranty Conditions

A new product purchased in the Alza.cz sales network is guaranteed for 2 years. If you need repair or other services during the warranty period, contact the product seller directly, you must provide the original proof of purchase with the date of purchase.

The following are considered to be a conflict with the warranty conditions, for which the claimed claim may not be recognized:

- Using the product for any purpose other than that for which the product is intended or failing to follow the instructions for maintenance, operation, and service of the product.
- Damage to the product by a natural disaster, the intervention of an unauthorized person or mechanically through the fault of the buyer (e.g., during transport, cleaning by inappropriate means, etc.).
- Natural wear and aging of consumables or components during use (such as batteries, etc.).
- Exposure to adverse external influences, such as sunlight and other radiation or electromagnetic fields, fluid intrusion, object intrusion, mains overvoltage, electrostatic discharge voltage (including lightning), faulty supply or input voltage and inappropriate polarity of this voltage, chemical processes such as used power supplies, etc.
- If anyone has made modifications, modifications, alterations to the design or adaptation to change or extend the functions of the product compared to the purchased design or use of non-original components.

Vážený zákazníku,

Děkujeme vám za zakoupení našeho produktu. Před prvním použitím si prosím pečlivě přečtěte následující pokyny a uschovejte si tento návod k použití pro budoucí použití. Zvláštní pozornost věnujte bezpečnostním pokynům. Pokud máte k přístroji jakékoli dotazy nebo připomínky, obraťte se na zákaznickou linku.

✉ www.alza.cz/kontakt

✆ +420 255 340 111

Dovozce Alza.cz a.s., Jankovcova 1522/53, Holešovice, 170 00 Praha 7, www.alza.cz

Úvod

CryptoMate EVO obsahuje kryptografický modul čipové karty ACOS5-EVO. Kryptografický modul čipové karty ACOS5-EVO nabízí pokročilé asymetrické a symetrické kryptografické algoritmy, například ECC a RSA, a je v souladu s mezinárodními standardy pro čipové karty PKI, například FIPS 14-2 (US Federal Information Processing Standards) Level 3 a CC EAL 5+ (úroveň čipu).

CryptoMate EVO má podobný vzhled jako CryptoMate Nano, ale po připojení k počítači jej lze snadno rozeznat podle zelené LED diody. Aplikace v PC jej rozpoznají podle názvu PCSC a názvu ovladače: ACS CryptoMate EVO. Ve srovnání s CryptoMate Nano nabízí také větší paměť a pokročilejší kryptografické funkce.

Funkce

Funkce kryptografických čipových karet

CryptoMate EVO obsahuje kryptografický modul čipové karty ACOS5-EVO, který má následující funkce:

Komunikační protokoly

- T=0, T=1 s přenosovou rychlostí až 446 400 bps

Paměť

- Kapacita: 192Kb
- Výdrž paměti EEPROM: 500 000 cyklů mazání/zápisu
- Uchovávání dat: 30 let

Kryptografické schopnosti

ACOS5-EVO podporuje řadu kryptografických algoritmů, včetně:

- ECC: Křivky P-224/P-256/P-384/P-521
- RSA: 512 - 4096 bitů v krocích po 256 bitech.
- AES: 128/192/256 bitů (ECB, CBC)
- DES/3DES: 56/112/168 bitů (ECB, CBC)
- Hash: SHA1, SHA224, SHA256, SHA384, SHA512
- MAC: CBC-MAC (DES/3DES, AES), CMAC (3DES, AES)

Generování náhodných čísel

- Deterministický RNG podle FIPS 140-2
- Nedeterministický RNG v souladu s AIS-31

Zabezpečení souborů

- Přístup ke čtení souborů se soukromými a tajnými klíči lze nastavit na hodnotu "Nikdy".
- Možnost podmíněného přístupu k souborům pomocí zabezpečeného atributu Compact v souladu s normou ISO 7816. Přístup k souboru je povolen pouze v případě, že jsou splněny příslušné bezpečnostní podmínky (např. předložení PIN).
- Schopnost splnění příkazové podmínky na vyhrazený soubor (DF) se zabezpečeným atributem v souladu s normou ISO 7816 - rozšířený. Příkazy jsou povoleny pouze v případě, že jsou splněny příslušné bezpečnostní podmínky (např. zadání PIN).
- Funkce Secure Messaging pro důvěrný a ověřený přenos dat
- Vzájemné ověřování (terminál-karta a karta-terminál) s generováním klíče relace pro šifrování a MAC.
- Podpora funkce proti vytržení

Dodržování norem

- Shoda s normami ISO 7816, části 1,2,3,4, 8 a 9.
- Soulad se standardem FIPS 140-2 úrovně 3
- Certifikováno podle Common Criteria ELA 5+ (úroveň čipu)

Funkce

Fyzické vlastnosti

- Zelená stavová LED dioda
- Nízká hmotnost: 4,61 g
- Extrémně malé rozměry: 29,25 mm x 14,80 mm x 10,28 mm
- Otvor na klíčenku
- Pouzdro s ochranou proti neoprávněné manipulaci
- Napájení čipové karty přes port USB

Dodržování norem

- Rozhraní USB s Full Speed
- Kompatibilní s CCID (Plug and Play)
- Certifikát CE a FCC
- V souladu s RoHS
- Certifikát REACH
- Certifikace Microsoft WHQL
- Podporuje systém Android 3.1 a novější

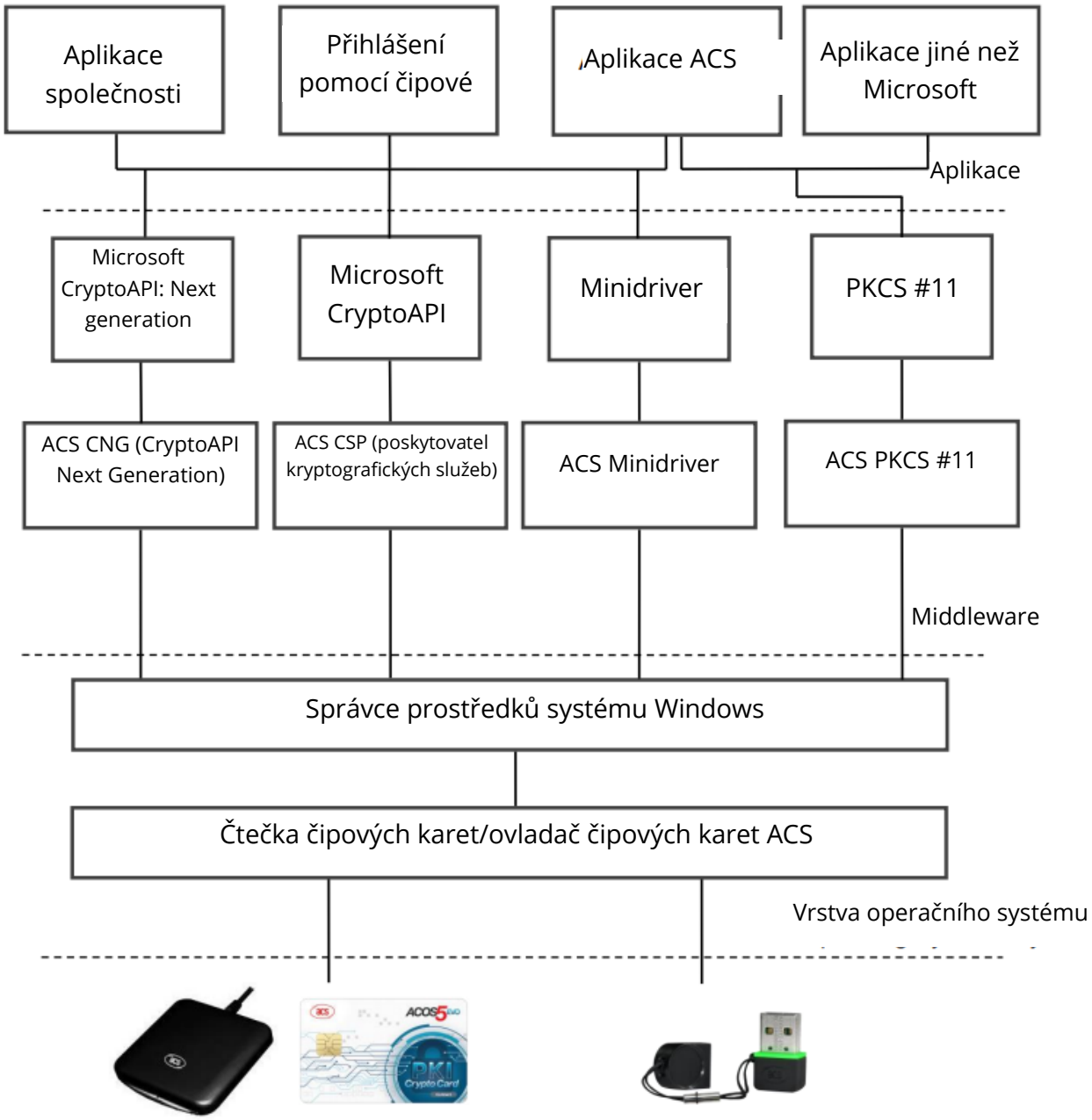
Typické aplikace

- e-Government
- e-Healthcare
- Bankovnictví a platby
- Zabezpečení sítě
- Řízení přístupu
- Infrastruktura veřejných klíčů
- Digitální podpis

Middleware

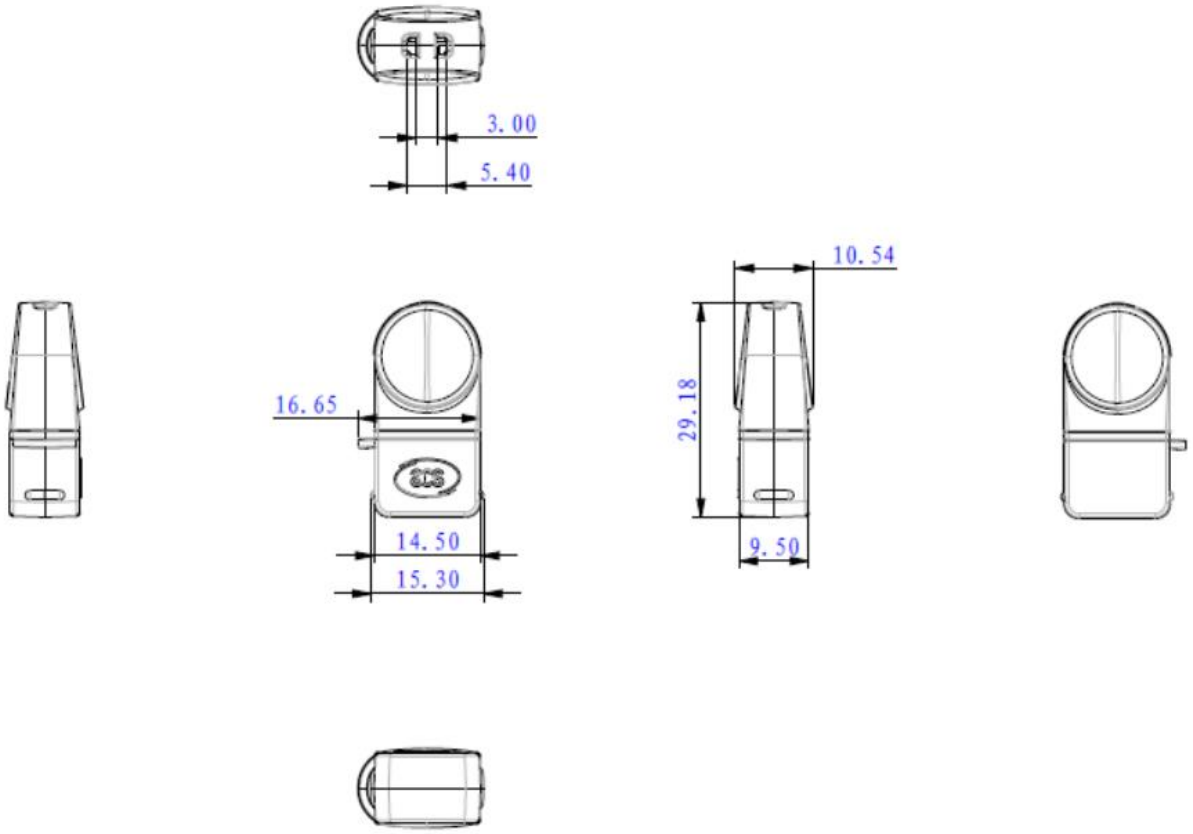
Pro použití CryptoMate EVO pro aplikace PKI s digitálními certifikáty je zapotřebí použitelný middleware id.

Společnost ACS nabízí softwarová řešení, jako je ACOS5 Minidriver a ACOS5-EVO PKI Kit, takže ACOS5-EVO a CryptoMate EVO lze používat s dalšími aplikacemi třetích stran, jak je znázorněno na obrázku níže:



V případě dotazů na podporu middlewaru pro token CryptoMate EVO nás prosím kontaktujte na adrese info@acs.com.hk.

Technické specifikace



Fyzické vlastnosti

Rozměry	29,18 mm (délka) x 14,50 mm (šířka) x 10,54 mm (výška)
Hmotnost	4.61 g
Barva	Černá

Modul kryptografické čipové karty ACOS5-EVO

Velikost paměti	192 KB
Výdrž	500 000 cyklů zápisu/vymazání
Uchovávání dat	30 let
Kryptografické schopnosti	ECC: Křivky P-224/P-256/P-384/P-521 RSA: AES: 512 - 4096 bitů v krocích po 256 bitech: DES/3DES: 128/192/256 bitů (ECB, CBC): MAC: 56/112/168 bitů (ECB, CBC): CBC-MAC (DES/3DES, AES) CMAC (3DES, AES)
Schopnost ukládání do paměti (Hashing Capabality)	SHA1, SHA 224, SHA256, SHA384, SHA512

Rozhraní USB Host

Protokol	USB CCID
Typ konektoru	Standardní typ A
Zdroj energie	Z portu USB
Rychlost	Full Speed USB (12 Mb/s)

Vestavěné periferie

LED	Zelená
Plášť	Zabezpečení proti neoprávněné manipulaci
Ostatní	Otvor na klíče pro přenášení

Provozní podmínky

Teplota	0°C - 50°C
Vlhkost	Max. 90 % (bez kondenzace)
MTBF	500 000 hodin

Certifikace/splnění požadavků

ISO 7816, USB Full Speed, Common Criteria ELA5+ (úroveň čipu), PC/SC, CCID, CE, FCC, RoHS, REACH, FIPS, 140-2 Level 3 (USA), Microsoft WHQL

Podpora middlewaru

ACS PKCS #11, ACS CSP (založený na CryptoAPI společnosti Microsoft), ACS CNG (založený na CNG společnosti Microsoft)
ACS Minidriver
X.509 v3 Certificate Storage (může ukládat více než 10 párů klíčů).

Podpora operačního systému ovladače zařízení

Windows 7, Windows 8, Windows 8.1, Windows 10
Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016
Linux, Mac OSM Android 3.1 a novější

Záruční podmínky

Na nový výrobek zakoupený v prodejní síti Alza.cz se vztahuje záruka 2 roky. V případě potřeby opravy nebo jiného servisu v záruční době se obraťte přímo na prodejce výrobku, je nutné předložit originální doklad o koupi s datem nákupu.

Za rozpor se záručními podmínkami, pro který nelze reklamaci uznat, se považují následující skutečnosti:

- Používání výrobku k jinému účelu, než pro který je výrobek určen, nebo nedodržování pokynů pro údržbu, provoz a servis výrobku.
- Poškození výrobku živelnou pohromou, zásahem neoprávněné osoby nebo mechanicky vinou kupujícího (např. při přepravě, čištění nevhodnými prostředky apod.).
- přirozené opotřebení a stárnutí spotřebního materiálu nebo součástí během používání (např. baterií atd.).
- Působení nepříznivých vnějších vlivů, jako je sluneční záření a jiné záření nebo elektromagnetické pole, vniknutí kapaliny, vniknutí předmětu, přepětí v síti, elektrostatický výboj (včetně blesku), vadné napájecí nebo vstupní napětí a nevhodná polarita tohoto napětí, chemické procesy, např. použité zdroje atd.

Pokud někdo provedl úpravy, modifikace, změny konstrukce nebo adaptace za účelem změny nebo rozšíření funkcí výrobku oproti zakoupené konstrukci nebo použití neoriginálních součástí.

Vážený zákazník,

ďakujeme vám za zakúpenie nášho výrobku. Pred prvým použitím si pozorne prečítajte nasledujúce pokyny a uschovajte si tento návod na použitie. Venujte osobitnú pozornosť bezpečnostným pokynom. Ak máte akékoľvek otázky alebo pripomienky k prístroju, obráťte sa na linku služieb zákazníkom.

✉ www.alza.sk/kontakt

✆ +421 257 101 800

Dovozca Alza.cz a.s., Jankovcova 1522/53, Holešovice, 170 00 Praha 7, www.alza.cz

Úvod

CryptoMate EVO obsahuje kryptografický modul čipovej karty ACOS5-EVO. Kryptografický modul čipovej karty ACOS5-EVO ponúka pokročilé asymetrické a symetrické kryptografické algoritmy, napríklad ECC a RSA, a je v súlade s medzinárodnými štandardmi pre čipové karty PKI, napríklad FIPS 14-2 (US Federal Information Processing Standards) Level 3 a CC EAL 5 + (úroveň čipu).

CryptoMate EVO má podobný vzhľad ako CryptoMate Nano, ale po pripojení k počítaču ho ľahko rozoznáte podľa zelenej LED diódy. Aplikácie v počítači ho rozpoznajú podľa názvu PCSC a názvu ovládača: ACS CryptoMate EVO. V porovnaní so zariadením CryptoMate Nano ponúka aj väčšiu pamäť a pokročilejšie kryptografické funkcie.

Funkcie

Funkcie kryptografických čipových kariet

CryptoMate EVO obsahuje kryptografický modul inteligentnej karty ACOS5-EVO, ktorý má tieto funkcie:

Komunikačné protokoly

- T=0, T=1 s prenosovými rýchlosťami do 446 400 bps

Pamäť

- Kapacita: 192Kb
- Životnosť pamäte EEPROM: 500 000 cyklov vymazania/zápisu
- Uchovávanie údajov: 30 rokov

Kryptografické zručnosti

ACOS5-EVO podporuje niekoľko kryptografických algoritmov vrátane:

- ECC: Krivky P-224/P-256/P-384/P-521
- RSA: 512 - 4096 bitov v krokoch po 256 bitoch.
- AES: 128/192/256 bitov (ECB, CBC)
- DES/3DES: 56/112/168 bitov (ECB, CBC)
- Hash: SHA1, SHA224, SHA256, SHA384, SHA512
- MAC: CBC-MAC (DES/3DES, AES), CMAC (3DES, AES)

Generovanie náhodných čísel

- Deterministický RNG podľa FIPS 140-2
- Nedeterministický RNG v súlade s AIS-31

Zabezpečenie súborov

- Prístup na čítanie súborov so súkromnými a tajnými kľúčmi je možné nastaviť na možnosť "Nikdy".
- Podmienený prístup k súborom je možný pomocou atribútu Secure Compact v súlade s normou ISO 7816. Prístup k súboru je povolený len vtedy, ak sú splnené príslušné bezpečnostné podmienky (napr. predloženie kódu PIN).
- Schopnosť splniť podmienku príkazu v súbore s obmedzeným prístupom (DF) so zabezpečeným atribútom v súlade s normou ISO 7816 - rozšírená. Príkazy sú povolené len vtedy, ak sú splnené príslušné bezpečnostné podmienky (napr. zadanie kódu PIN).
- Zabezpečené posielanie správ na dôverný a overený prenos údajov
- Vzájomná autentifikácia (terminál-karta a karta-terminál) s generovaním kľúča relácie na šifrovanie a MAC.
- Podpora funkcie proti roztrhnutiu

Dodržiavanie noriem

- Súlad s normou ISO 7816, časti 1,2,3,4, 8 a 9.
- Súlad so štandardom FIPS 140-2 úrovne 3
- Certifikované podľa Common Criteria ELA 5+ (úroveň čipu)

Funkcie čipov

Fyzikálne vlastnosti

- Zelená stavová LED dióda
- Nízka hmotnosť: 4,61 g
- Extrémne malé rozmery: 29,25 mm x 14,80 mm x 10,28 mm
- Otvor na kľúčenku
- Puzdro odolné proti neoprávnenej manipulácii
- Napájanie čipovej karty cez port USB

Dodržiavanie noriem

- Rozhranie USB s plnou rýchlosťou
- Kompatibilita s CCID (Plug and Play)
- Certifikácia CE a FCC
- Zhoda s RoHS
- Certifikát REACH
- Certifikácia Microsoft WHQL
- Podpora systému Android 3.1 a novších verzií

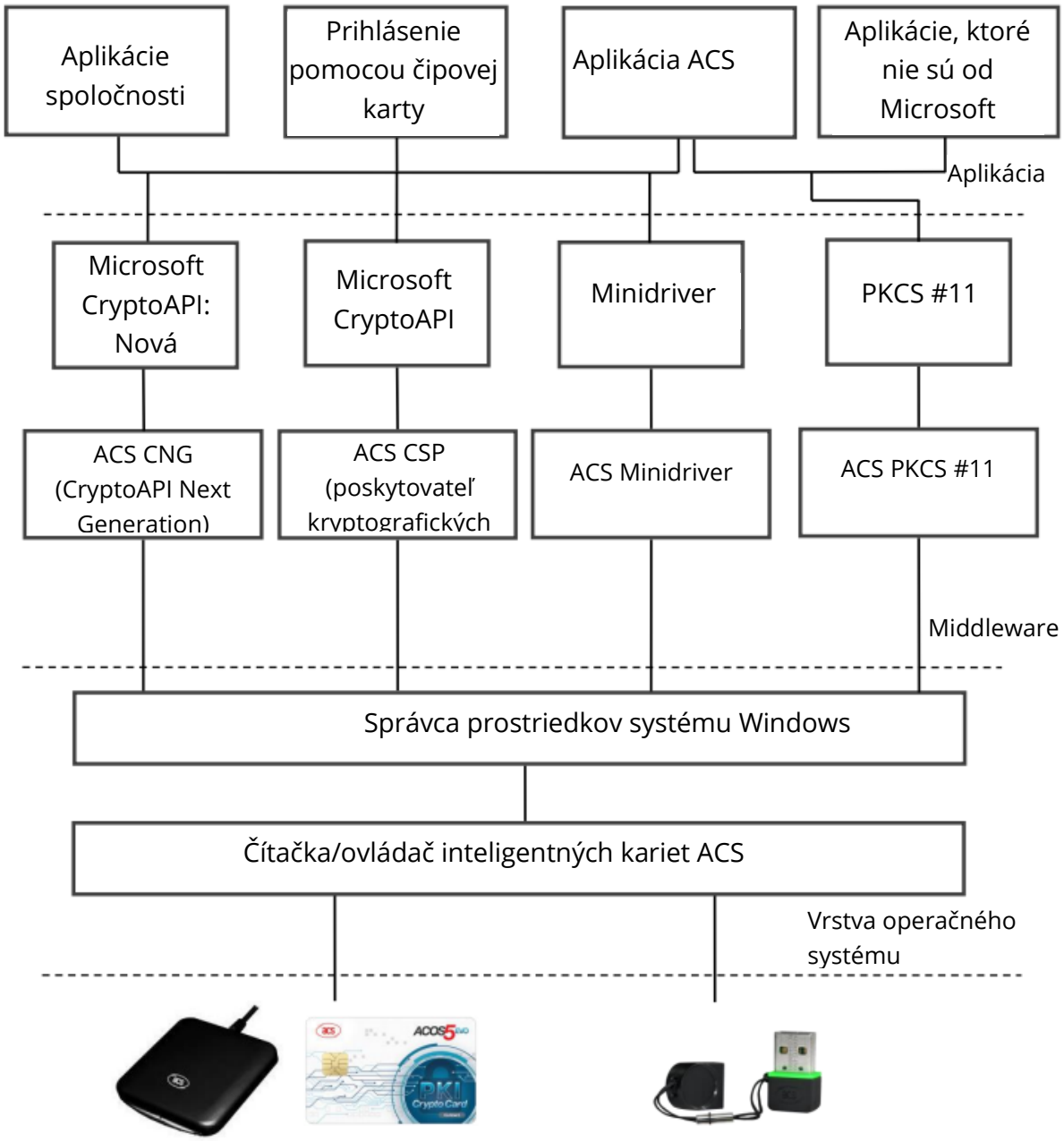
Typické aplikácie

- e-Government
- Elektronická zdravotná starostlivosť
- Bankovníctvo a platby
- Zabezpečenie siete
- Kontrola prístupu
- Infraštruktúra verejného kľúča
- Digitálny podpis

Middleware

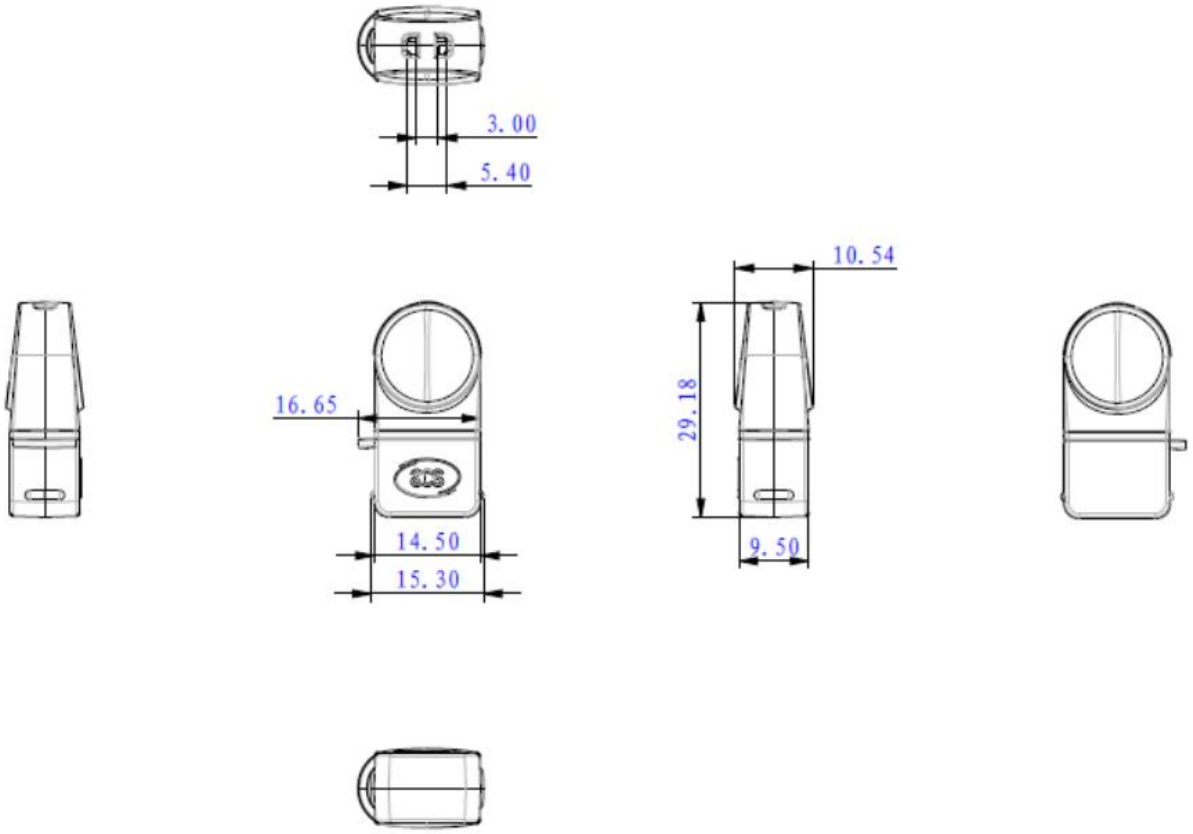
Na používanie CryptoMate EVO pre aplikácie PKI s digitálnymi certifikátmi je potrebný použiteľný middleware id.

Spoločnosť ACS ponúka softvérové riešenia, ako napríklad ACOS5 Minidriver a ACOS5-EVO PKI Kit, takže ACOS5-EVO a CryptoMate EVO možno používať s inými aplikáciami tretích strán, ako je znázornené na obrázku nižšie:



V prípade otázok týkajúcich sa podpory middlevéru pre token CryptoMate EVO nás kontaktujte na adrese info@acs.com.hk.

Technická špecifikácia



Fyzikálne vlastnosti

Rozmery	29,18 mm (dĺžka) x 14,50 mm (šírka) x 10,54 mm (výška)
Hmotnosť	4.61 g
Farba	Čierna

Modul kryptografickej čipovej karty ACOS5-EVO

Veľkosť pamäte	192 KB
Vytrvalosť	500 000 cyklov zápisu/vymazania
Uchovávanie dát	30 rokov
Kryptografické zručnosti	ECC: Krivky P-224/P-256/P-384/P-521 RSA: AES: 512 - 4096 bitov v 256-bitových krokoch: DES/3DES: 128/192/256 bitov (ECB, CBC): MAC: 56/112/168 bitov (ECB, CBC): CBC-MAC (DES/3DES, AES) CMAC (3DES, AES)
Schopnosť ukladania do pamäti (Hashing Capabality)	SHA1, SHA 224, SHA256, SHA384, SHA512

Rozhranie USB Host

Protokol	USB CCID
Typ konektora	Štandardný typ A
Zdroj energie	Z portu USB
Rýchlosť	Plná rýchlosť USB (12 Mb/s)

Zabudované periférie

LED	Zelená
Plášť	Zabezpečenie proti neoprávnenej manipulácii
Iné	Kľúčová dierka na prenášanie

Prevádzkové podmienky

Teplota	0°C - 50°C
Vlhkosť	Max. 90 % (bez kondenzácie)
MTBF	500 000 hodín

Certifikácia/splnenie požiadaviek

ISO 7816, USB Full Speed, Common Criteria ELA5+ (úroveň čipu), PC/SC, CCID, CE, FCC, RoHS, REACH, FIPS, 140-2 Level 3 (USA), Microsoft WHQL

Podpora middleware

ACS PKCS #11, ACS CSP (založený na Microsoft CryptoAPI), ACS CNG (založený na Microsoft CNG)
ACS Minidriver X.
509 v3 Certificate Storage (môže uchovávať viac ako 10 párov kľúčov).

Podpora operačného systému ovládača zariadenia

Windows 7, Windows 8, Windows 8.1, Windows 10
Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016
Linux, Mac OSM Android 3.1 a novší

Záručné podmienky

Na nový výrobok zakúpený v predajnej sieti Alza.sk sa vzťahuje záruka 2 roky. V prípade potreby opravy alebo iného servisu v záručnej dobe sa obráťte priamo na predajcu výrobku, je nutné predložiť originálny doklad o kúpe s dátumom nákupu.

Za rozpor so záručnými podmienkami, pre ktorý nemožno reklamáciu uznať, sa považujú nasledujúce skutočnosti:

- Používanie výrobku na iný účel, než na ktorý je výrobok určený alebo nedodržiavanie pokynov pre údržbu, prevádzku a servis výrobku.
- Poškodenie výrobku živelnou pohromou, zásahom neoprávnenej osoby alebo mechanicky vinou kupujúceho (napr. pri preprave, čistení nevhodnými prostriedkami a pod.).
- Prirodzené opotrebovanie a starnutie spotrebného materiálu alebo súčastí počas používania (napr. batérií atď.).
- Pôsobenie nepriaznivých vonkajších vplyvov, ako je slnečné žiarenie a iné žiarenie alebo elektromagnetické pole, vniknutie kvapaliny, vniknutie predmetu, prepätie v sieti, elektrostatický výboj (vrátane blesku), chybné napájacie alebo vstupné napätie a nevhodná polarita tohto napätia, chemické procesy, napr. použité zdroje atď.

Ak niekto vykonal úpravy, modifikácie, zmeny konštrukcie alebo adaptácie za účelom zmeny alebo rozšírenia funkcií výrobku oproti zakúpenej konštrukcii alebo použitie neoriginálnych súčastí.

Kedves vásárló,

Köszönjük, hogy megvásárolta termékünket. Kérjük, az első használat előtt figyelmesen olvassa el az alábbi utasításokat, és őrizze meg ezt a használati útmutatót a későbbi használatra. Fordítson különös figyelmet a biztonsági utasításokra. Ha bármilyen kérdése vagy észrevétele van a készülékkel kapcsolatban, kérjük, forduljon az ügyfélvonalhoz.

✉ www.alza.hu/kapcsolat

✆ +36-1-701-1111

Importőr Alza.cz a.s., Jankovcova 1522/53, Holešovice, 170 00 Prága 7, www.alza.cz

Bevezetés

A CryptoMate EVO egy ACOS5-EVO kriptográfiai intelligens kártyamodult tartalmaz. Az ACOS5-EVO kriptográfiai intelligens kártyamodul fejlett aszimmetrikus és szimmetrikus kriptográfiai algoritmusokat, például ECC-t és RSA-t kínál, és megfelel a PKI intelligens kártyákra vonatkozó nemzetközi szabványoknak, például a FIPS 14-2 (US Federal Information Processing Standards) Level 3 és a CC EAL 5+ (chipszint) szabványoknak.

A CryptoMate EVO megjelenésében hasonlít a CryptoMate Nano készülékhez, de a számítógépbe csatlakoztatva könnyen megkülönböztethető a zöld LED segítségével. A PC-alkalmazások a PCSC és az illesztőprogram neve alapján ismerik fel: ACS CryptoMate EVO. A CryptoMate Nano készülékhez képest nagyobb memóriával és fejlettebb kriptográfiai funkciókkal rendelkezik.

Jellemzők

Titkosított intelligens kártya jellemzői

A CryptoMate EVO tartalmazza az ACOS5-EVO kriptográfiai intelligens kártyamodult, amely a következő jellemzőkkel rendelkezik:

Kommunikációs protokollok

- T=0, T=1 446 400 bps-ig terjedő bauddal

Memória

- Kapacitás: 192Kb
- EEPROM tartósság: törlési/írási ciklusok: 500.000
- Adatmegőrzés: 30 év

Kriptográfiai képességek

Az ACOS5-EVO számos kriptográfiai algoritmust támogat, többek között:

- ECC: P-224/P-256/P-384/P-521 görbék
- RSA: bitek 256 bites lépésekben.
- AES: (ECB, CBC): 128/192/256 bit (ECB, CBC)
- DES/3DES: 56/112/168 bit (ECB, CBC)
- Hash: SHA1, SHA224, SHA256, SHA384, SHA512
- MAC: CBC-MAC (DES/3DES, AES), CMAC (3DES, AES)

Véletlenszám generálás

- Determinisztikus RNG a FIPS 140-2 szerint
- Az AIS-31 szabványnak megfelelő nemdeterminisztikus RNG

Fájlbiztonság

- A privát és titkos kulcsfájlok olvasási hozzáférése beállítható "Soha" értékre.
- Fájlhozzáférési feltételrendszer az ISO 7816 szabványnak megfelelő Secure Attribute-Compact funkcióval. A fájlhozzáférés csak akkor engedélyezett, ha a megfelelő biztonsági feltételek teljesülnek (pl. PIN-kód beadása).
- Parancsvégrehajtási feltételképesség dedikált fájlonként (DF) ISO 7816-kompatibilis kiterjesztett biztonságos attribútummal. A parancsok csak akkor engedélyezettek, ha a megfelelő biztonsági feltételek teljesülnek (pl. PIN-kód megadása).
- Biztonságos üzenetküldési funkció a bizalmas és hitelesített adatátvitelhez
- Kölcsönös hitelesítés (terminál-kártya és kártya-terminál között), a titkosításhoz és a MAC-hez szükséges munkamenetkulcs generálásával.
- Anti-tearing funkció támogatása

A szabványoknak való megfelelés

- Megfelel az ISO 7816 1., 2.3.3., 4., 8. és 9. részének.
- Megfelelés a FIPS 140-2 3. szintnek
- Common Criteria ELA 5+ (Chip szint) tanúsítvánnyal rendelkezik.

Token jellemzők

Fizikai jellemzők

- Zöld állapot LED
- Könnyű súly: 4,61 g
- Rendkívül kicsi: 29,25 mm x 14,80 mm x 10,28 mm
- Kulcstartó lyuk
- Szabotázsbiztos burkolat
- Intelligens kártya tápellátása USB porton keresztül

A szabványoknak való megfelelés

- Teljes sebességű USB interfész
- CCID-kompatibilis (Plug and Play)
- CE és FCC tanúsítvánnyal
- RoHS-konform
- REACH tanúsítvánnyal rendelkező
- Microsoft WHQL-tanúsítvány
- Támogatja az Android 3.1 és újabb verziókat

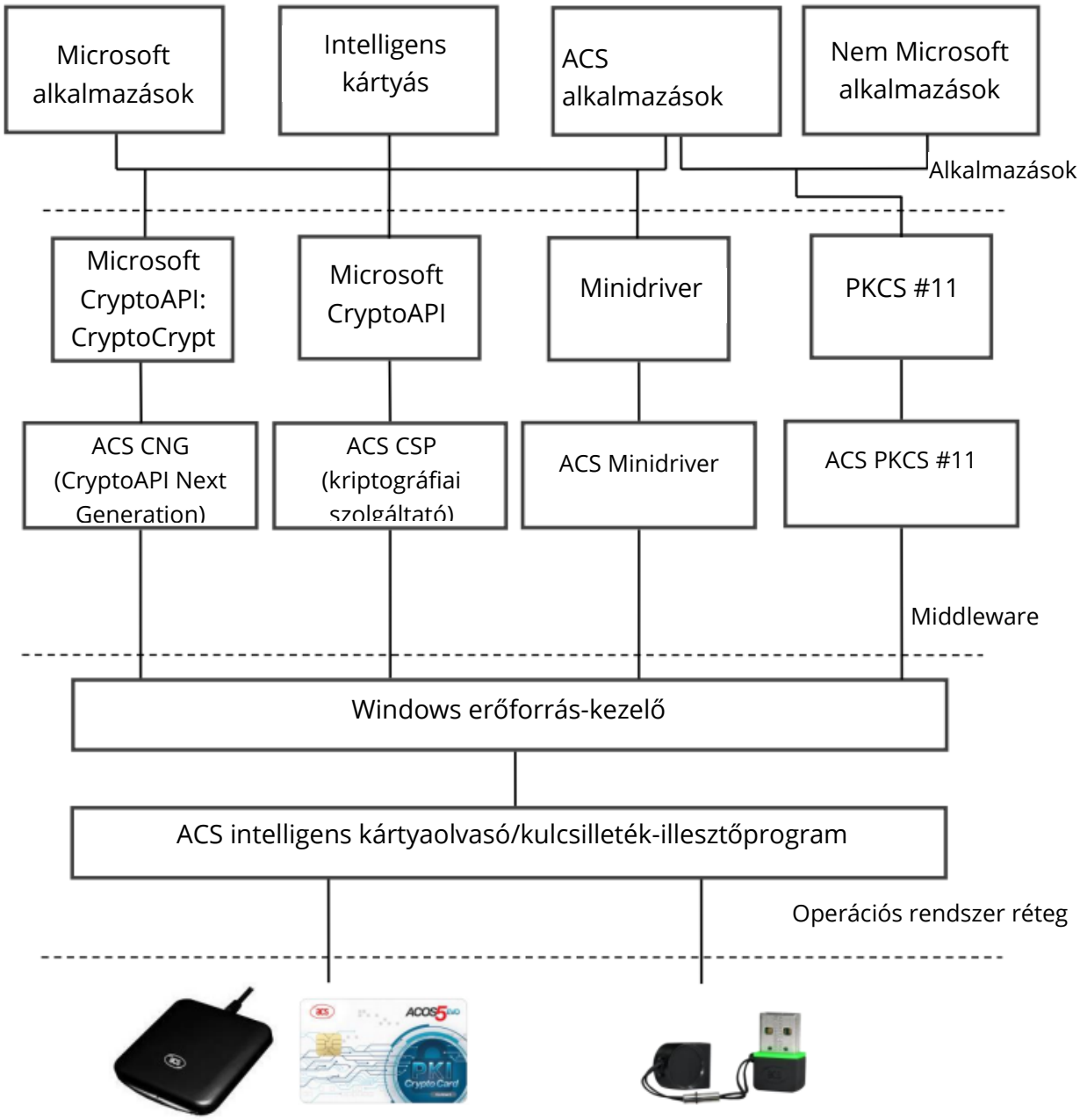
Tipikus alkalmazások

- E-kormányzat
- E-egészségügy
- Banki és fizetési szolgáltatások
- Hálózati biztonság
- Hozzáférés-ellenőrzés
- Nyilvános kulcsú infrastruktúra
- Digitális aláírás

Middleware

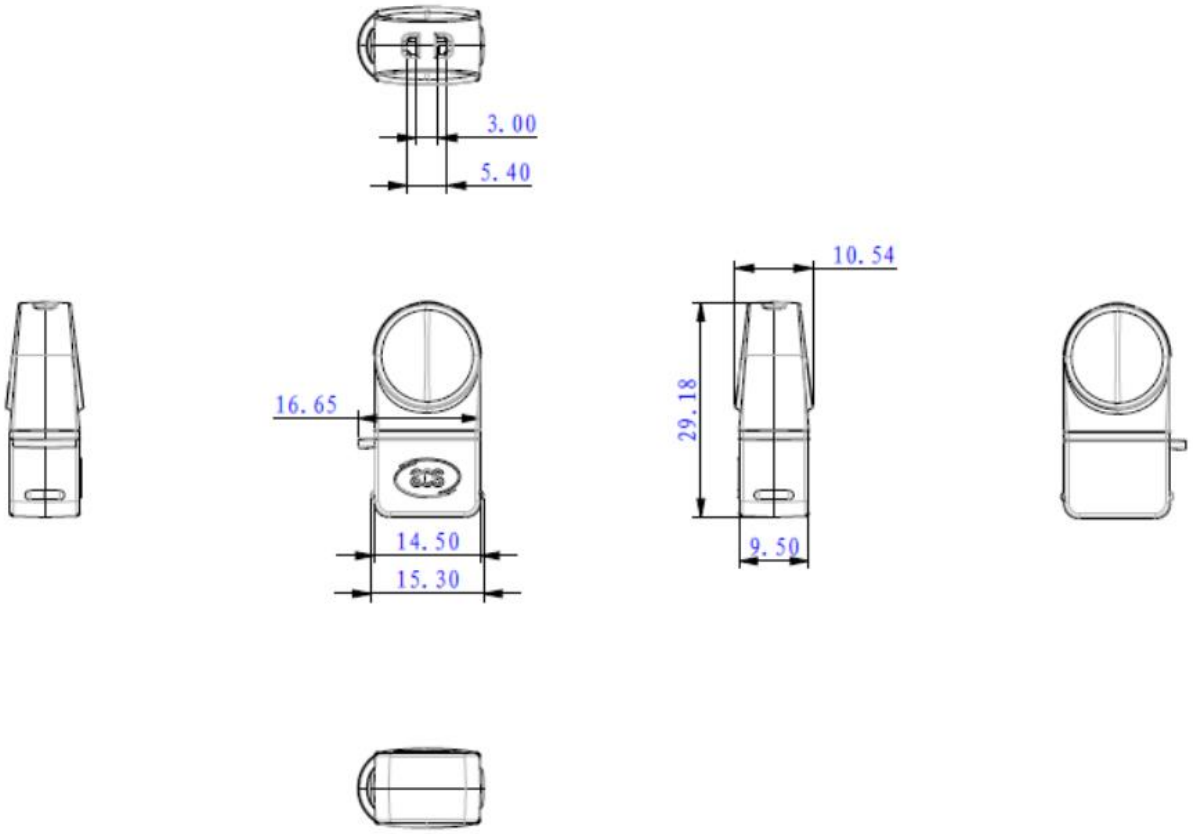
A CryptoMate EVO digitális tanúsítványokkal rendelkező PKI-alkalmazásokhoz való használatához egy megfelelő middleware id szükséges.

Az ACS olyan szoftveres megoldásokat kínál, mint az ACOS5 Minidriver és az ACOS5-EVO PKI Kit, hogy az ACOS5-EVO és a CryptoMate EVO más, harmadik féltől származó alkalmazásokkal is használható legyen, ahogy az alábbi ábrán látható:



A CryptoMate EVO token middleware-támogatásával kapcsolatos kérdéseivel forduljon hozzánk a info@acs.com.hk e-mail címen.

Műszaki specifikációk



Fizikai jellemzők

Méretek	29,18 mm (hosszúság) x 14,50 mm (szélesség) x 10,54 mm (magasság)
Súly	4.61 g
Szín	Fekete

ACOS5-EVO kriptográfiai intelligens kártyamodul

Memória mérete	192 KB
Állóképesség	500 000 írási/törlési ciklus
Adatmegőrzés	30 év
Kriptográfiai képesség	ECC: P-224/P-256/P-384/P-521 RSA: AES: 512 - 4096 bit 256 bites lépésekben: (ECB, CBC) DES/3DES: 128/192/256 bit (ECB, CBC) DES/3DES: 128/192/256 bit: (ECB, CBC) MAC: 56/112/168 bit (ECB, CBC): CBC-MAC (DES/3DES, AES) CMAC (3DES, AES)
Hashtalanítási képesség	SHA1, SHA 224, SHA256, SHA384, SHA512

USB Host interfész

Jegyzőkönyv	USB CCID
Csatlakozó típusa	Standard A típus
Energiaforrás	USB portról
Sebesség	Teljes sebességű USB (12 Mbps)

Beépített perifériák

LED	Zöld
Burkolat	Szabotázsbiztos
Egyéb	Keychan lyuk a hordozhatóság érdekében

Működési feltételek

Hőmérséklet	0°C - 50°C
Páratartalom	Max. 90% (nem kondenzáló)
MTBF	500,000 óra

Tanúsítványok/megfelelőség

ISO 7816, USB Full Speed, Common Criteria ELA5+ (Chip Level), PC/SC, CCID, CE, FCC, RoHS, REACH, FIPS, 140-2 Level 3 (USA), Microsoft WHQL

Middleware támogatás

ACS PKCS #11, ACS CSP (a Microsoft CryptoAPI-n alapul), ACS CNG (a Microsoft CNG-n alapul)
ACS Minidriver
X.509 v3 tanúsítványtárolás (több mint 10 kulcspár tárolására képes).

Eszközillesztő-program operációs rendszer támogatása

Windows 7, Windows 8, Windows 8.1, Windows 10
Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016
Linux, Mac OSM Android 3.1 és újabb verziók

Jótállási feltételek

Az Alza.cz értékesítési hálózatában vásárolt új termékre 2 év garancia vonatkozik. Ha a garanciális időszak alatt javításra vagy egyéb szolgáltatásra van szüksége, forduljon közvetlenül a termék eladójához, a vásárlás dátumával ellátott eredeti vásárlási bizonylatot kell bemutatnia.

Az alábbiak a jótállási feltételekkel való ellentétnek minősülnek, amelyek miatt az igényelt követelés nem ismerhető el:

- A terméknek a termék rendeltetésétől eltérő célra történő használata, vagy a termék karbantartására, üzemeltetésére és szervizelésére vonatkozó utasítások be nem tartása.
- A termék természeti katasztrófa, illetéktelen személy beavatkozása vagy a vevő hibájából bekövetkezett mechanikai sérülése (pl. szállítás, nem megfelelő eszközökkel történő tisztítás stb. során).
- A fogyóeszközök vagy alkatrészek természetes elhasználódása és öregedése a használat során (pl. akkumulátorok stb.).
- Káros külső hatásoknak való kitettség, például napfény és egyéb sugárzás vagy elektromágneses mezők, folyadék behatolása, tárgyak behatolása, hálózati túlfeszültség, elektrosztatikus kisülési feszültség (beleértve a villámlást), hibás táp- vagy bemeneti feszültség és e feszültség nem megfelelő polaritása, kémiai folyamatok, például használt tápegységek stb.

Ha valaki a termék funkcióinak megváltoztatása vagy bővítése érdekében a megvásárolt konstrukcióhoz képest módosításokat, átalakításokat, változtatásokat végzett a konstrukción vagy adaptációt végzett, vagy nem eredeti alkatrészeket használt.

Sehr geehrter Kunde,

vielen Dank für den Kauf unseres Produkts. Bitte lesen Sie die folgenden Anweisungen vor dem ersten Gebrauch sorgfältig durch und bewahren Sie diese Bedienungsanleitung zum späteren Nachschlagen auf. Beachten Sie insbesondere die Sicherheitshinweise. Wenn Sie Fragen oder Kommentare zum Gerät haben, wenden Sie sich bitte an den Kundenservice.

✉ www.alza.de/kontakt

✆ 0800 181 45 44

✉ www.alza.at/kontakt

✆ +43 720 815 999

Lieferant Alza.cz a.s., Jankovcova 1522/53, Holešovice, 170 00 Prag 7, www.alza.cz

Einführung

Der CryptoMate EVO enthält ein kryptografisches Smartcard-Modul ACOS5-EVO. Das kryptografische Smartcard-Modul ACOS5-EVO bietet fortschrittliche asymmetrische und symmetrische kryptografische Algorithmen wie ECC und RSA und entspricht internationalen Standards für PKI-Smartcards wie FIPS 14-2 (US Federal Information Processing Standards) Level 3 und CC EAL 5+ (Chiplevel).

Der CryptoMate EVO sieht ähnlich aus wie der CryptoMate Nano, ist aber durch seine grüne LED leicht zu erkennen, wenn er an den PC angeschlossen ist. PC-Anwendungen erkennen ihn an seinem PCSC und dem Treibernamen: ACS CryptoMate EVO. Außerdem bietet er im Vergleich zum CryptoMate Nano einen größeren Speicher und fortschrittlichere kryptografische Funktionen.

Eigenschaften

Kryptographische Smart Card Merkmale

Das CryptoMate EVO enthält das kryptografische Chipkartenmodul ACOS5-EVO mit den folgenden Merkmalen:

Kommunikationsprotokolle

- T=0, T=1 mit Baud bis zu 446.400 bps

Speicher

- Kapazität: 192Kb
- EEPROM-Ausdauer: 500.000 Schreib-/Löschzyklen
- Datenaufbewahrung: 30 Jahre

Kryptographische Fähigkeiten

Der ACOS5-EVO unterstützt eine Reihe von kryptographischen Algorithmen, darunter:

- ECC: Kurven P-224/P-256/P-384/P-521
- RSA: 512 - 4096 Bits in 256-Bit-Schritten
- AES: 128/192/256-Bit (ECB, CBC)
- DES/3DES: 56/112/168-Bits (ECB, CBC)
- Hash: SHA1, SHA224, SHA256, SHA384, SHA512
- MAC: CBC-MAC (DES/3DES, AES), CMAC (3DES, AES)

Erzeugung von Zufallszahlen

- Deterministischer RNG gemäß FIPS 140-2
- Nicht-deterministischer RNG gemäß AIS-31

Datei-Sicherheit

- Der Lesezugriff auf private und geheime Schlüsseldateien kann auf "Nie" gesetzt werden.
- Möglichkeit des Dateizugriffs mit ISO 7816-kompatiblen Secure Attribute-Compact. Der Dateizugriff ist nur erlaubt, wenn die entsprechenden Sicherheitsbedingungen erfüllt sind (z. B. PIN-Eingaben)
- Fähigkeit zur Befehlsausführungsbedingung pro Dedicated File (DF) mit ISO 7816-konformer Secure Attribute-Extended. Befehle sind nur zulässig, wenn die entsprechenden Sicherheitsbedingungen erfüllt sind (z. B. PIN-Eingabe)
- Secure Messaging-Funktion für vertrauliche und authentifizierte Datenübertragung
- Gegenseitige Authentifizierung (Terminal-zu-Karte und Karte-zu-Terminal) mit Erzeugung von Sitzungsschlüsseln für Verschlüsselung und MAC
- Unterstützung der Anti-Tearing-Funktion

Einhaltung von Normen

- Übereinstimmung mit ISO 7816 Teile 1, 2, 3, 4, 8 und 9
- Übereinstimmung mit FIPS 140-2 Level 3
- Zertifiziert mit Common Criteria ELA 5+ (Chip Level)

Token-Merkmale

Physikalische Merkmale

- Grüne Status-LED
- Leichtgewicht: 4,61 g
- Äußerst klein: 29,25 mm x 14,80 mm x 10,28 mm
- Loch für Schlüsselanhänger
- Originalitätsgesichertes Gehäuse
- Stromversorgung der Chipkarte über USB-Anschluss

Einhaltung von Normen

- USB-Vollgeschwindigkeitsschnittstelle
- CCID-konform (Plug and Play)
- CE- und FCC-zertifiziert
- RoHS-konform
- REACH-zertifiziert
- Microsoft WHQL-zertifiziert
- Unterstützt Android 3.1 und höher

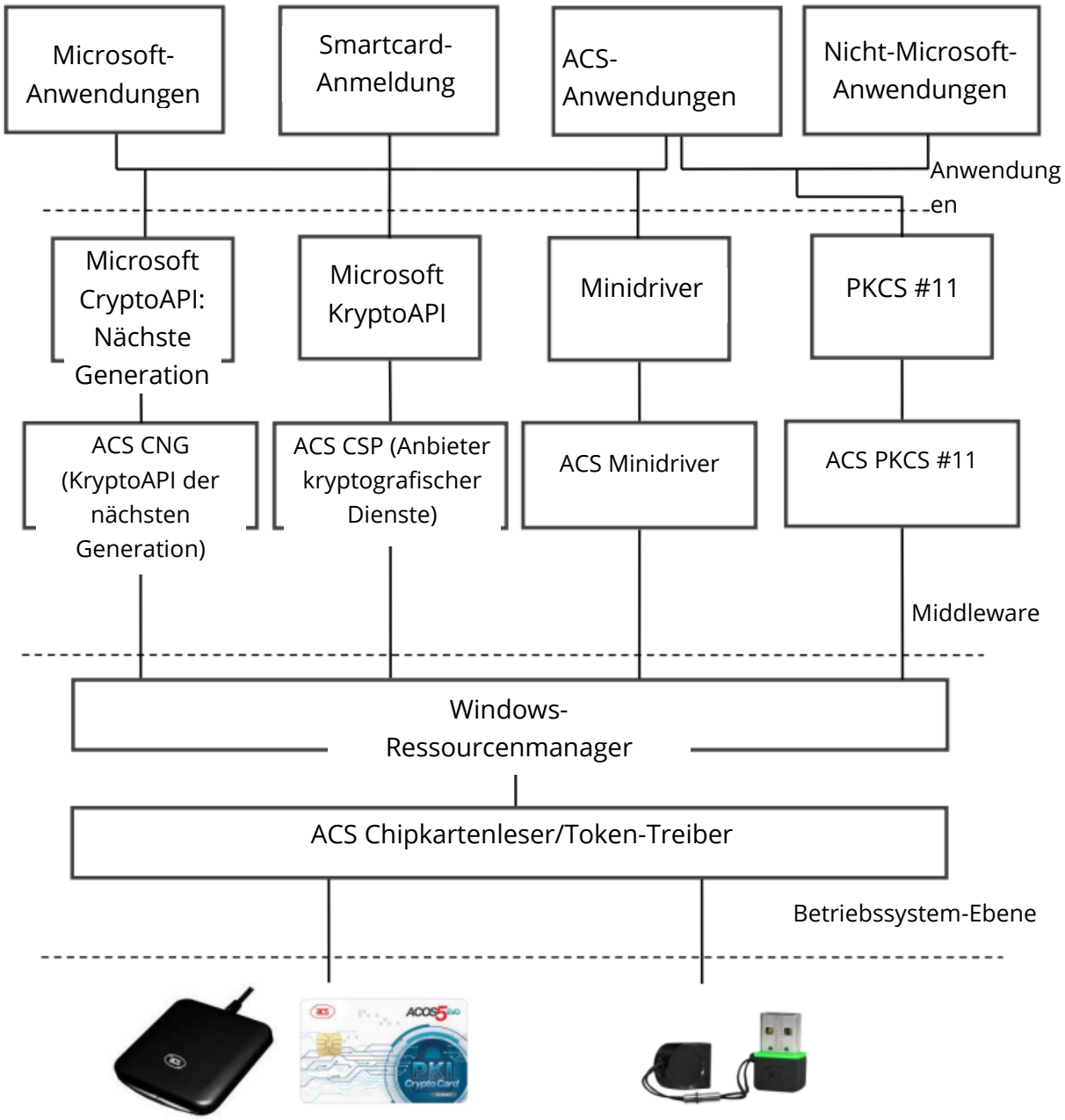
Typische Anwendungen

- E-Government
- Elektronische Gesundheitsdienste
- Bankwesen und Zahlungen
- Netzwerksicherheit
- Zugangskontrolle
- Infrastruktur für öffentliche Schlüssel
- Digitale Unterschrift

Middleware

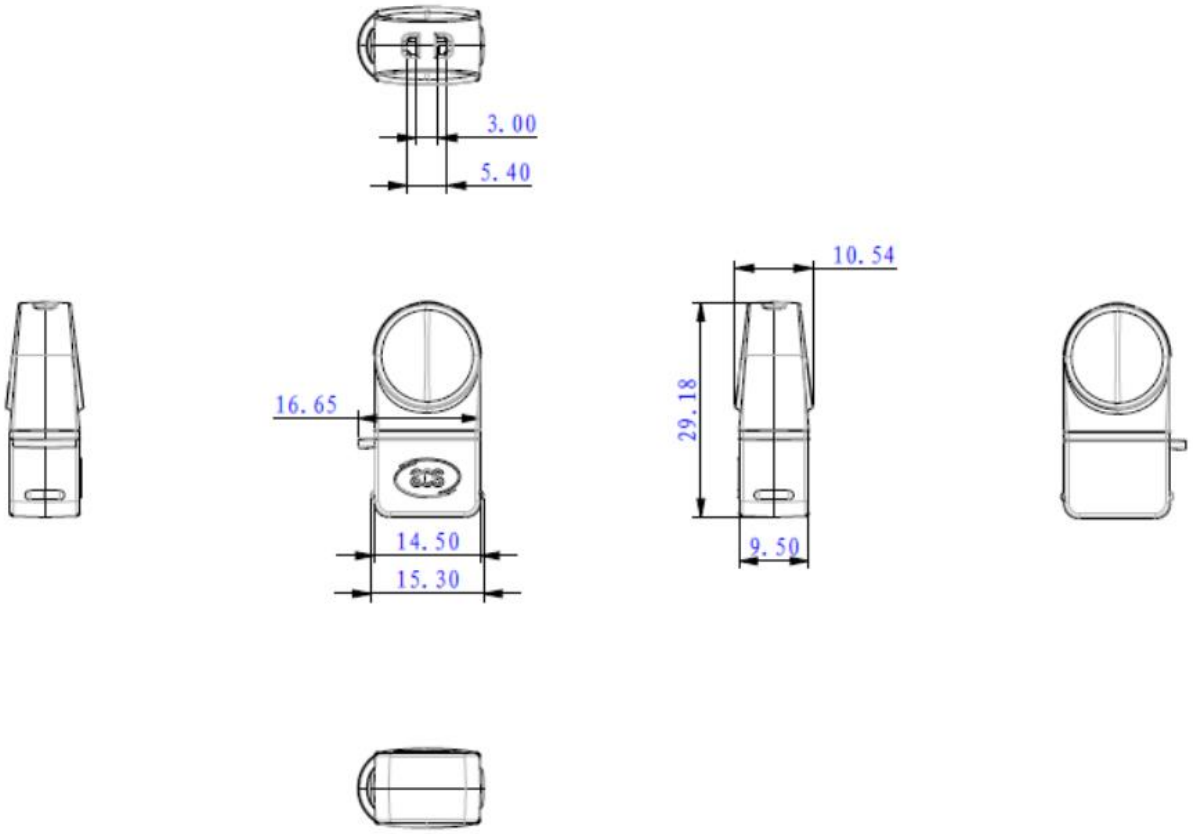
Um CryptoMate EVO für PKI-Anwendungen mit digitalen Zertifikaten zu nutzen, wird eine entsprechende Middleware benötigt.

ACS bietet Softwarelösungen wie den ACOS5 Minidriver und das ACOS5-EVO PKI Kit an, so dass der ACOS5-EVO und der CryptoMate EVO mit anderen Anwendungen von Drittanbietern verwendet werden können, wie in der Abbildung unten dargestellt:



Bitte kontaktieren Sie uns unter info@acs.com.hk für Anfragen bezüglich der Middleware-Unterstützung für den CryptoMate EVO-Token.

Technische Daten



Physikalische Merkmale

Abmessungen	29,18 mm (L) x 14,50 mm (B) x 10,54 mm (H)
Gewicht	4.61 g
Farbe	Schwarz

ACOS5-EVO Kryptografisches Chipkartenmodul

Speichergröße	192 KB
Ausdauer	500.000 Schreib-/Löschzyklen
Aufbewahrung von Daten	30 Jahre
Kryptographische Fähigkeit	ECC: Kurven P-224/P-256/P-384/P-521 RSA: 512 - 4096 Bits in 256-Bit-Schritten AES: 128/192/256-Bits (ECB, CBC) DES/3DES: 56/112/168 Bits (ECB, CBC) MAC: CBC-MAC (DES/3DES, AES) CMAC (3DES, AES)
Hashing-Fähigkeit	SHA1, SHA 224, SHA256, SHA384, SHA512

USB-Host-Schnittstelle

Protokoll	USB CCID
Stecker Typ	Standard Typ A
Stromquelle	Vom USB-Anschluss
Geschwindigkeit	USB Volle Geschwindigkeit (12 Mbps)

Eingebaute Peripheriegeräte

LED	Grün
Gehäuse	Manipulationssicherung
Andere	Schlüsselloch für Tragbarkeit

Betriebsbedingungen

Temperatur	0°C - 50°C
Luftfeuchtigkeit	Max. 90% (nicht kondensierend)
MTBF	500.000 Stunden

Zertifizierungen/Konformität

ISO 7816, USB Full Speed, Common Criteria ELA5+ (Chip Level), PC/SC, CCID, CE, FCC, RoHS, REACH, FIPS, 140-2 Level 3 (USA), Microsoft WHQL

Middleware-Unterstützung

ACS PKCS #11, ACS CSP (basierend auf Microsofts CryptoAPI), ACS CNG (basierend auf Microsofts CNG)
ACS Minidriver
X.509 v3 Zertifikatsspeicher (kann mehr als 10 Schlüsselpaare speichern)

Gerätetreiber-Betriebssystem-Unterstützung

Windows 7, Windows 8, Windows 8.1, Windows 10
Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016
Linux, Mac OSM Android 3.1 und höher

Garantiebedingungen

Auf ein neues Produkt, das im Vertriebsnetz von Alza gekauft wurde, wird eine Garantie von 2 Jahren gewährt. Wenn Sie während der Garantiezeit eine Reparatur oder andere Dienstleistungen benötigen, wenden Sie sich direkt an den Produktverkäufer. Sie müssen den Originalkaufbeleg mit dem Kaufdatum vorlegen.

Als Widerspruch zu den Garantiebedingungen, für die der geltend gemachte Anspruch nicht anerkannt werden kann, gelten:

- Verwendung des Produkts für einen anderen Zweck als den, für den das Produkt bestimmt ist, oder Nichtbeachtung der Anweisungen für Wartung, Betrieb und Service des Produkts.
- Beschädigung des Produkts durch Naturkatastrophe, Eingriff einer unbefugten Person oder mechanisch durch Verschulden des Käufers (z.B. beim Transport, Reinigung mit unsachgemäßen Mitteln usw.).
- Natürlicher Verschleiß und Alterung von Verbrauchsmaterialien oder Komponenten während des Gebrauchs (wie Batterien usw.).
- Einwirkung schädlicher äußerer Einflüsse wie Sonnenlicht und anderen Strahlungen oder elektromagnetischen Feldern, Eindringen von Flüssigkeiten, Eindringen von Gegenständen, Netzüberspannung, elektrostatische Entladungsspannung (einschließlich Blitzschlag), fehlerhafte Versorgungs- oder Eingangsspannung und falsche Polarität dieser Spannung, chemische Prozesse wie verwendet Netzteile usw.

Wenn jemand Änderungen, Modifikationen, Konstruktionsänderungen oder Anpassungen vorgenommen hat, um die Funktionen des Produkts gegenüber der gekauften Konstruktion zu ändern oder zu erweitern oder nicht originale Komponenten zu verwenden.