

Životný cyklus a správa kryptografických klíčů v praxi

 martin.rublik@gmail.com



 [@martin_rublik](https://twitter.com/martin_rublik)

 <https://www.linkedin.com/in/mrublik/>

O mne

- Martin Rublík
 - FMFI UK
 - Študent 😊
 - EUBA FHI
 - Doktorand, asistent (2009-2014)
 - BSP Consulting
 - Konzultant (2005 - \$(get-date))
- Špecializácie 😎
 - Microsoft Cloud / On-Premise
 - Autentifikácia a autorizácia
 - IAM/IdM
 - Cloud security
 - PKI (CA/TSA/RA, čipové karty, HSM, ...)
- Zľahka 😊
 - Sieťová bezpečnosť
 - Analýza rizík / riadenie rizík

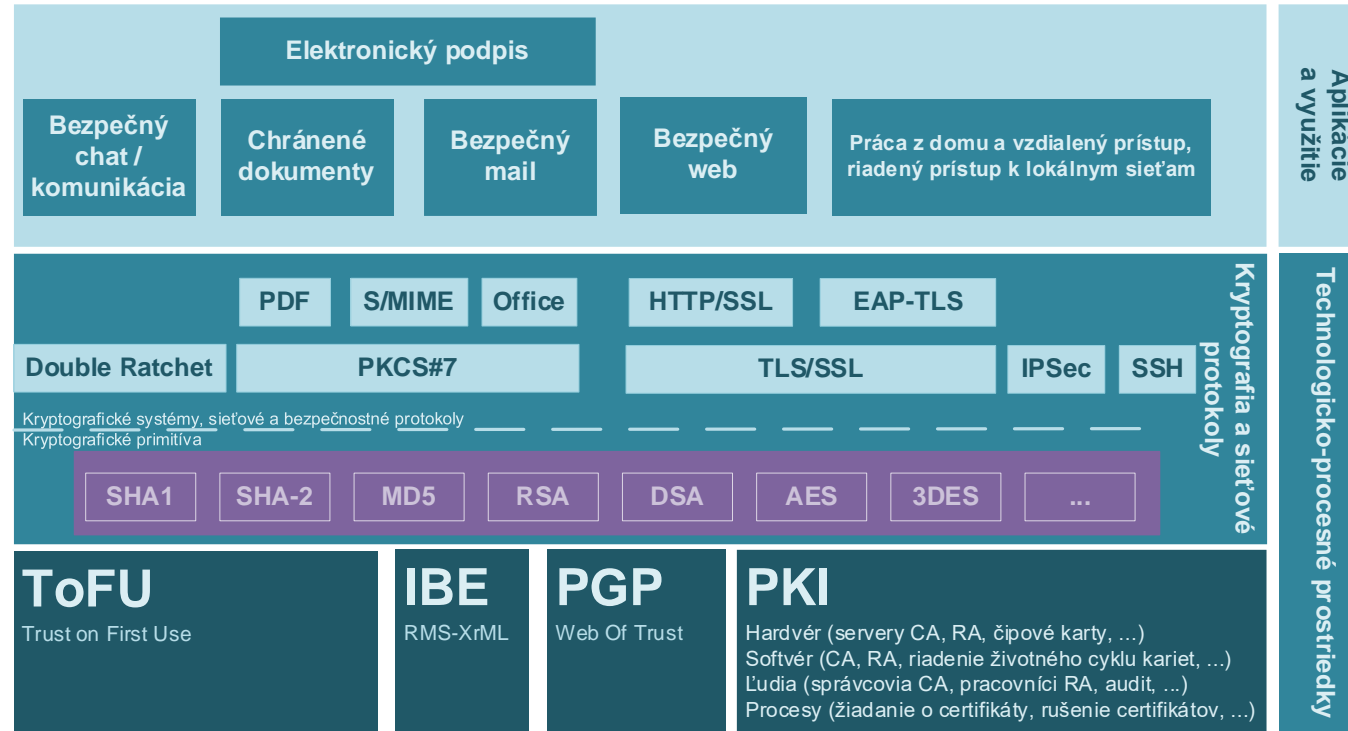
Agenda

- Úvod
- Životný cyklus kryptografických kľúčov
 - Prehľad
 - Aspekty správy kryptografických kľúčov
 - Riziká spojené s kryptografickými kľúčmi
 - Možnosti uloženia a ochrana kryptografických kľúčov
- Demo  

Úvod

Využitie kryptografie a aspekty jej bezpečnosti

- Kryptografia využitie
 - Integrita
 - Autentifikácia, nepopierateľnosť
 - Dôvernosť
- Matematické
 - Algoritmy, Protokoly, ...
- Inžinierske
 - Štandardizácia, Architektúra, Implementácia,
 - ...
- Procesné
 - Previazanie identity
 - Distribúcia kľúčov
 - ...



Úvod Závislosti

- Bezpečnosť kryptografie \neq {dĺžka kľúča, AES, SHA2, ...}
 - [\(Gutmann, et al.\) The Curse of Cryptography Numerology](#)

So, rather than making us more secure, the focus on cryptographic numerology falls afoul of the law of unintended consequences. Concentrating on fighting the threat of numerically endowed foreign powers makes us significantly less secure by excluding the use of SSL-everywhere

- [\(Lenstra, et al.\) Universal Security; From bits and mips to pools, lakes -and beyond](#)

...

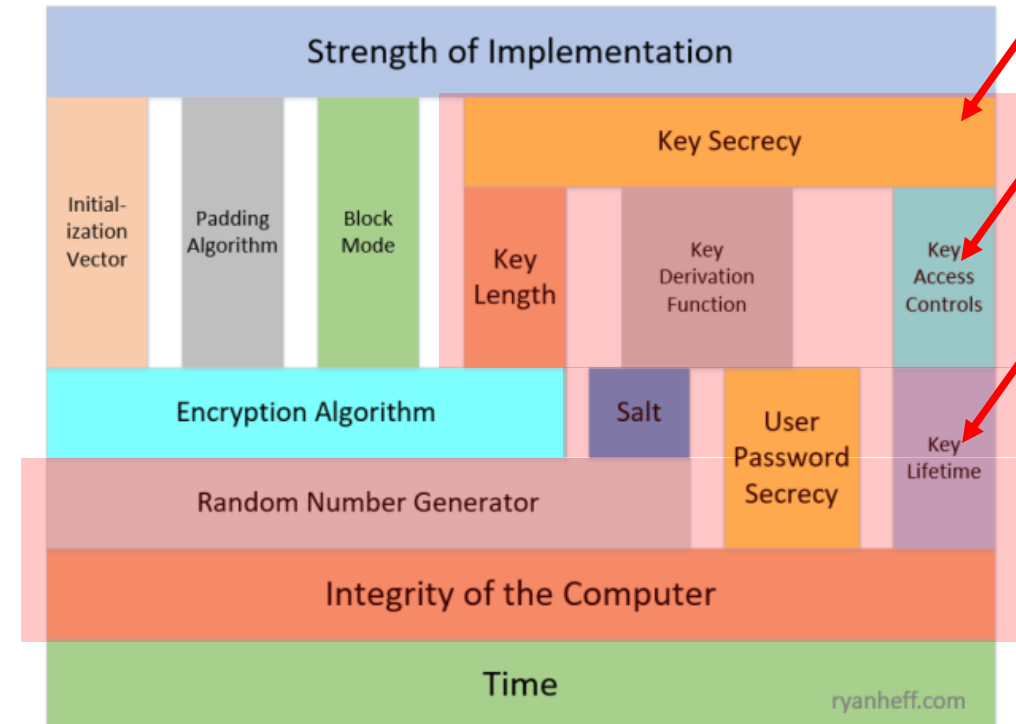
The problem is that for all these cryptosystems key length and security level are measured in bits, but that the relationship between the two varies wildly – from trivial, to simple, to rather contrived.

... The new approach was inspired by a remark made by the third author during his presentation of the factorization of the 768-bit RSA challenge at Crypto 2010: We estimate that the energy required for the factorization would have sufficed to bring two 20°C Olympic size swimming pools to a boil.

... Boiling all water on the planet (including all starfish) amounts to about 224 lakes of Geneva and leads to global security: 114-bit symmetric cryptosystems, 228-bit cryptographic hashes, and 2380-bit RSA.

Cryptosystem Dependencies

Encryption is about far more than key length and algorithm choice. In this diagram, each box is dependent on those below it. This is an oversimplification that doesn't represent all cryptosystems (it uses AES as an example), but it should make you think about the factors involved. See ryanheff.com/2018/01/10/crypto for guidance.



<https://ryanheff.wordpress.com/2018/01/10/crypto/>

Table 1. Intuitive security levels.

security level	volume of water to bring to a boil	bit-lengths		
		symmetric key	cryptographic hash	RSA modulus
teaspoon security	0.0025 liter	35	70	242
shower security	80 liter	50	100	453
pool security	2 500 000 liter	65	130	745
rain security	0.082 km ³	80	160	1130
lake security	89 km ³	90	180	1440
sea security	3 750 000 km ³	105	210	1990
global security	1 400 000 000 km ³	114	228	2380
solar security	-	140	280	3730

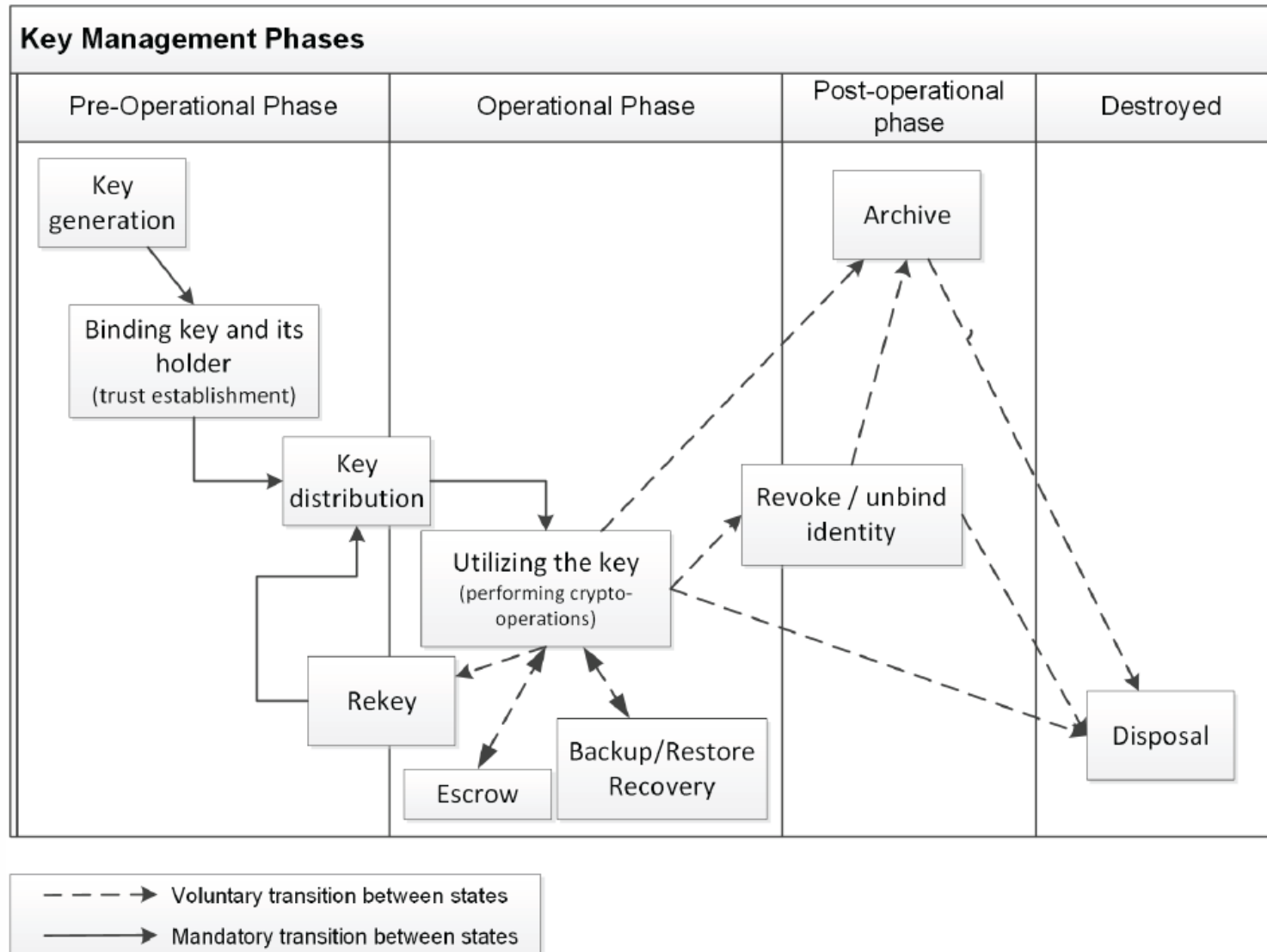
Životný cyklus kryptografických kľúčov

Typy kryptografických kľúčov

- V závislosti od typu používaného systému
 - Symetrické
 - Asymetrické
- V závislosti od predpokladanej doby ich využitia
 - Dlhodobé
 - Krátkodobé
- V závislosti od ich účelu
 - Šifrovanie údajov
 - Šifrovanie ďalších kľúčov
 - Digitálny podpis údajov / dokumentov
 - Autentifikácia
- V závislosti od možnosti ich využitia
 - Autentifikácia (server side, client side, mutual, user, API, ...)
 - Dôvernosť (Ochrana elektronickej pošty, šifrovanie dokumentov, šifrovanie údajov na pevných diskoch)
 - Nepopierateľnosť (elektronický podpis)
 - Kombinácia (pozor)

Životný cyklus kryptografických klíčů

Fázy životného cyklu



Životný cyklus kryptografických kľúčov

Požiadavky / aspekty správy kryptografických kľúčov

- Bezpečné generovanie kľúčov
- Zložitosť distribúcie a zviazania/rozviazania s držiteľom
- Bezpečné použitie a uloženie
 - Bezpečnej zálohy a obnovy držiteľom
 - Podmienenej/kontrolovanej obnovy treťou stranou (key escrow)
 - Použitia na viacerých zariadeniach / operačných systémoch
 - Ochrana pred držiteľom 😊 (export / import, napr. [DRM](#) alebo popretie autorstva)
- Možnosti automatizácie správy
- Audit prístupu ku kľúču a jeho použitia v celom životnom cykle

Životný cyklus kryptografických kľúčov

Požiadavky v kontexte fáz

Security service Key management phase affected	Authentication	Data Confidentiality	Non-repudiation
Key generation	Sufficient assurance that the private key can be used only by its holder should be provided.	Key generation should be done in a secure way that prevents the attacker from gaining access to private key.	High assurance that the private key can be used only by its holder must be provided.
Binding key and its holder's identity	The binding should provide a unique link to the holder's identity (with respect to information systems that make use of authentication service). Pseudonyms can be used.	Unique link to holder's identity is not required. Pseudonyms can be used.	Holder's identity and cryptographic keys should be associated in a legally binding way. Pseudonyms should not be used unless clearly marked and traceable.
Escrow / Key Recovery	Key escrow/recovery SHOULD NOT be used.	Key escrow/recovery might be desirable especially in enterprise environments.	Key escrow/recovery MUST NOT be used.
Backup and restore	Key backup and restore is not crucial for user auth. For trust anchors extremely important.	Key backup and restore is important especially for protecting data-at-rest.	Key backup and restore is not crucial.
Revocation (Unbinding the holder's identity)	Revocation service or keys with short lifetime might be necessary to deal with key compromise (protection against impersonation attacks).	Revocation service or keys with short lifetime are necessary deal with key compromise (protection against man-in-the-middle and impersonation attacks).	Timely revocation service is necessary deal with key lost and compromise situations (protection against impersonation and repudiation attacks). Archive records of revocation information might be needed

Životný cyklus kryptografických kľúčov

Hrozby

- Kompromitácia kľúča
 - „Slabá sila“ kľúča
 - Únik kľúča
 - Krádež kľúča / zneužitie kľúča
- Dočasná alebo trvalá nedostupnosť kľúča
 - Chyba v konfigurácii
 - Následok kompromitácie
 - Chyba v SW/HW

Životný cyklus kryptografických kľúčov

Slabá sila kľúča

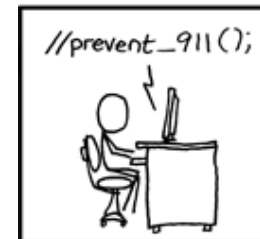
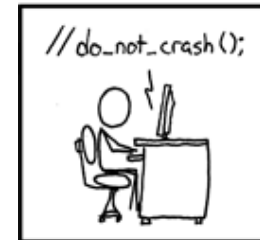
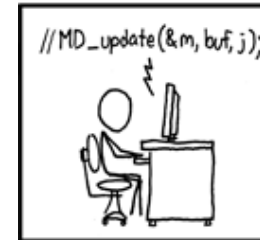
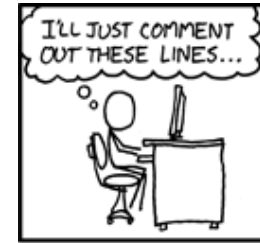
- Predsa len malá dĺžka kľúča 😊
 - [~ 2010 – SSL Observatory](#)
 - identifikovalo EV TLS certifikáty s dĺžkou kľúča [512 bitov](#) a iné chyby s ohľadom na X.509 internet PKI
- Chyba pri generovaní kľúčov (slabá entropia, chyba v algoritme)
 - pri prezeraní verejne dostupnej DB RSA verejných kľúčov SSL Observatory ~ 2010

RSA Exponent	Spolu	Duplicitné (total)	Duplicitné v %	Skupiny
65537	1 353 597	13 097	1%	3191
17	23 692	8	0%	4
3	493	24	5%	8
5	212	2	1%	1
7	97	0	0%	0

Životný cyklus kryptografických kľúčov

Slabá sila kľúča

- Chyba v generovaní kľúčov (nízka entropia, chyba v algoritme na generovanie, backdoor ...)
 - ~ [2008 - Debian weak key generation bug](#) (v [openssl patch-i](#)) entropia kľúčov bola výrazne nižšia, chyba bola prítomná cca 2 roky
 - ~ [2006](#), [2007](#), [2013](#) – Dual_EC_DRBG generátor náhodných čísiel pre eliptické krivky,
 - ~ [2017 – ROCA](#) chyba v generovaní kľúčov v rozličných knižniciach, ale aj HW,
 - možnosť faktorizácie do 3och mesiacov,
 - odhadovaná cena faktorizácie 2048 bitového RSA kľúča \$20,000-\$40,000
 - Okrem iného dopad na estónske aj slovenské eID
- Ochrana
 - **Byť pripravený na túto možnosť, najmä ak sa jedná o dôležité systémy**
 - Pokiaľ možno, používať štandardné produkty a frameworky
 - CC/FIPS certifikácia dá istú informáciu o kvalite produktu a spôsobe vývoja, týmto chybám však nemusí zamedziť (viď ROCA)



IN THE RUSH TO CLEAN UP THE DEBIAN-OPENSSL FIASCO, A NUMBER OF OTHER MAJOR SECURITY HOLES HAVE BEEN UNCOVERED:

AFFECTED SYSTEM	SECURITY PROBLEM
FEDORA CORE	VULNERABLE TO CERTAIN DECODER RINGS
XANDROS (EEE PC)	GIVES ROOT ACCESS IF ASKED IN STERN VOICE
GENTOO	VULNERABLE TO FLATTERY
OLPC OS	VULNERABLE TO JEFF GOLDBLUM'S POWERBOOK
SLACKWARE	GIVES ROOT ACCESS IF USER SAYS ELVISH WORD FOR "FRIEND"
UBUNTU	URNS OUT DISTRO IS ACTUALLY JUST WINDOWS VISTA WITH A FEW CUSTOM THEMES

Životný cyklus kryptografických kľúčov Únik kľúča

- Neplánované zverejnenie kľúčov (ale aj hesiel, a pod.)
 - V zdrojovom kóde
 - (verejne) dostupné repozitáre, napr. GitHub
 - V konfiguračných súboroch
 - (verejne) dostupné fóra
 - V zle nakonfigurovaných serveroch
 - (verejne) (neautentifikovane) dostupné servery
- Ochrana
 - Správny konfiguračný manažment
 - „Vyňatie“ citlivých údajov zo zdrojových kódov a konfigurácie
 - Použitie iných mechanizmov ako súbory na správu kľúčov

RECOVERING A FULL PEM PRIVATE KEY WHEN HALF OF IT IS REDACTED

Mar 24, 2021 • CryptoHackers

The [@CryptoHack__](#) account was pinged today by ENOENT, with a CTF-like challenge found in the wild: [Source tweet](#). Here's a write-up covering how given a partially redacted PEM, the whole private key can be recovered. The Twitter user, SAXX, shared a partially redacted private RSA key in a tweet about a penetration test where they had recovered a private key. Precisely, a screenshot of a PEM was shared online with 31 of 51 total lines of the file redacted.




Životný cyklus kryptografických kľúčov

Krádež / zneužitie kľúča

- Krádež
 - Po kompromitácii systému môže útočník kľúče **exportovať** a **využiť aj neskôr**
 - Krádež býva ťažko detekovateľná pretože audit prístupu ku kryptografickým kľúčom nie je bežnou praxou
 - Ukradnutý kľúč môže predstavovať ideálny backdoor, často umožňuje prístup na ľubovoľnej úrovni najmä ak sa jedná o kľúče IdP alebo certifikačných autorít, útočník má potenciálne dlhý prístup k systému
- Zneužitie
 - Po kompromitácii systému môže útočník kľúče používať po dobu prístupu k systému, bez auditnej stopy (**napr. vydať si certifikát ktorý nie je súčasťou DB certifikačnej autority**)
 - Po kompromitácii systému môže útočník pristupovať k službe a získať napr. certifikáty avšak tieto budú evidované v rámci DB certifikačnej autority
- Spracovanie/analýza auditných záznamov býva náročná
- Príklady
 - [~ 2020 Solorigate](#) – útočníci po úvodnej kompromitácii systému získali certifikáty a privátne kľúče IdP čím dokázali predstierať identitu používateľov v rámci O365
 - [~ 2011 DigiNotar](#) – útočníci [kompromitovali](#) CA DigiNotar, podarilo sa im vydať certifikáty ktoré neskôr boli využité v MITM útoku (Google/Iran)
- Techniky a referencie
 - <https://attack.mitre.org/techniques/T1552/>
 - <https://o365blog.com/post/adfs/>
 - <https://www.sans.org/webcasts/defending-your-cloud-against-ad-fs-attacks/>
- Ochrana
 - Obmedzenie prístupu a správne prístupové práva
 - Použitie ďalšej vrstvy ochrany či už na úrovni softvéru (KeyVault, Hashicorp Vault, ...) alebo hardvéru (HSM, čipové karty, TPM, ...)
 - [Key Usage Counting](#) (v závislosti od implementácie vie byť náročné na udržiavanie a sledovanie)

Životný cyklus kryptografických kľúčov

(dočasná) nedostupnosť kľúča

- Nedostupnosť kľúča spôsobí (katastrofálne) výpadky
 - [~ 2009 – HSM outage causes root CA key loss](#) – Strata kľúča pre e-gesundsheitKarte (našťastie v testovacej prevádzke ovplyvnených < 1.000 používateľov)
 - Key Rollover (vydanie nového certifikátu s novým kľúčom) môže mať za následok výraznú zmenu
 - Interná CA a množstvo zariadení o ktorých možno už nikto nič netuší
 - IdP a naviazané aplikácie s otáznou podporou viacerých podpisových kľúčov 
 - Množstvo príkladov z praxe ...
- Ochrana
 - Návrh systému tak aby bol čo najmenej náchylný na výpadok
 - Plánovanie na výpadok
 - Odstránenie „single point of failure“
 - Automatizácia / user friendly konfigurácia služieb
 - Konfiguračný manažment a dôkladná komunikácia zmien
 - Zálohy / obnovy a ich pravidelné testovanie

Uloženie a používanie kľúčov

Súbory

- PKCS#1 (a.k.a --- BEGIN RSA PRIVATE KEY ---)
 - Základný formát pre RSA kľúča
- PKCS#8 (a.k.a --- BEGIN PRIVATE KEY ---)
 - Pridáva podporu iných typov kľúčov
 - Umožňuje šifrovanie kľúča
- PKCS#12 (p12, pfx)
 - Umožňuje prenos privátneho kľúča aj certifikátu (ov) v rámci jedného súboru
- Java Key Store (jks)
 - Umožňuje uložiť a štruktúrovať viacero privátnych kľúčov a certifikátov v rámci jedného súboru
- Ochrana
 - Na základe ACL
 - Na základe hesla (heslo býva však zvyčajne súčasťou konfiguračného súboru)
- Výhody
 - Jednoduchosť
 - Prenositeľnosť
 - Ľahký backup / restore
- Riziká
 - Náročnejší konfiguračný manažment
 - Jednoduchá kompromitácia

Uloženie a používanie kľúčov

Windows certificate stores I.

- Current User
 - Špecifické per používateľ
- Local Machine
 - Špecifické per server / pracovná stanica
 - Zvyčajne sa využíva pre služby alebo pre autentifikáciu serveru resp. pracovnej stanice
 - Niektoré časti (Root resp. CA) sú implicitne skopírované do Current User store
- Zaujímavé časti
 - My (Personal)
 - Root (Trusted Root Certification Authorities)
 - CA (Intermediate Certification Authorities)
 - Certifikáty podriadených certifikačných autorít
 - Slúži na **zjednodušenie distribúcie** nie na zaistenie dôvery
 - TrustedPeople (Trusted People)
 - Explicitne dôveryhodné certifikáty (nekontroluje sa ich platnosť)

Uloženie a používanie kľúčov

Windows certificate stores II.

- Lokálne / Registry

- CurrentUser

- %AppData%\Microsoft\SystemCertificates\My\Certificates
HKCU\SOFTWARE\Microsoft\SystemCertificates

- LocalMachine

- HKLM\SOFTWARE\Microsoft\SystemCertificates
CERTUTIL -viewstore

- GPO

- HKLM\SOFTWARE\Policies\Microsoft\SystemCertificates
CERTUTIL -viewstore -groupolicy

- AD

- CERTUTIL -viewstore -enterprise
 - CERTUTIL -DSPublish
 - NTAUTH Store

Certificates Snap-in	Enterprise PKI Snap-in	CERTUTIL Command	Registry
Trusted Root Certification Authorities	Certificates Authorities Container tab	Root	Root
Intermediate Certification Authorities	AIA Container tab	SubCA (publish to AD) CA (View local store)	CA
Third-Party Root Certification Authorities	not applicable	AuthRoot	AuthRoot
Personal	not applicable	MY	MY
not applicable	NTAuthCertificates tab	NTAuthCA (publish to AD) NTAuth (View)	not applicable

Uloženie a používanie kľúčov

Windows certificate stores III.

- Kľúče
 - Registry
 - LocalMachine
 - HKLM\SOFTWARE\Microsoft\SystemCertificates\My\Keys
 - CurrentUser
 - HKCU\SOFTWARE\Microsoft\SystemCertificates\My\Keys
 - LocalMachine
 - LocalSystem
 - %ProgramData%\Microsoft\Crypto\RSA\MachineKeys
 - CurrentUser
 - %AppData%\Microsoft\SystemCertificates\My\Keys\

Uloženie a používanie kľúčov

Windows certificate stores IV.

- Ochrana

- DPAPI

- CryptProtectData / CryptUnprotectData
 - RPC local call -> lsass.exe

- Export flag

- DWORD value (0/1), stored together with private key
 - Encrypted by DPAPI

- CRYPTPROTECT_PROMPTSTRUCT

- Prístupové práva možno priradiť aj cez súborový systém odporúča sa však použiť MMC konzola alebo PS

When the `CRYPTPROTECT_PROMPTSTRUCT` is passed to `CryptProtectData()` or the internal protect function, the table below lists the defined flag values.

When the `CRYPTPROTECT_PROMPTSTRUCT` is passed to `CryptUnprotectData()` or the internal unprotect function, no flag values are defined.

<code>CRYPTPROTECT_PROMPT_ON_PROTECT</code>	Prompt on protect and unprotect.
<code>CRYPTPROTECT_PROMPT_ON_UNPROTECT</code>	Prompt on protect and unprotect.
<code>CRYPTPROTECT_STRONG</code>	Set the default user security level to strong.

Uloženie a používanie kľúčov

Windows certificate stores V.

- Výhody

- Nižšie riziko náhodného úniku privátnych kľúčov (tie obyčajne nie sú hardkódované v zdrojových súboroch)
- Istá miera ochrany pomocou DPAPI
- ADCS / jednoduchá distribúcia certifikátov

- Riziká

- Zložitejšia záloha / obnova certifikátov
- Potenciálne zložitejšie na automatizáciu
- ADCS služba náročná na [správne](#) nasadenie a [konfiguráciu](#)
- Po vymazaní certifikátu cez MMC konzolu sa nemaže príslušný privátny kľúč
- Neexportovateľné certifikáty sú exportovateľné
 - Mimikatz / iSEC Partners Jailbreak
 - Pri žiadosti o certifikát môže používateľ zmeniť tento parameter

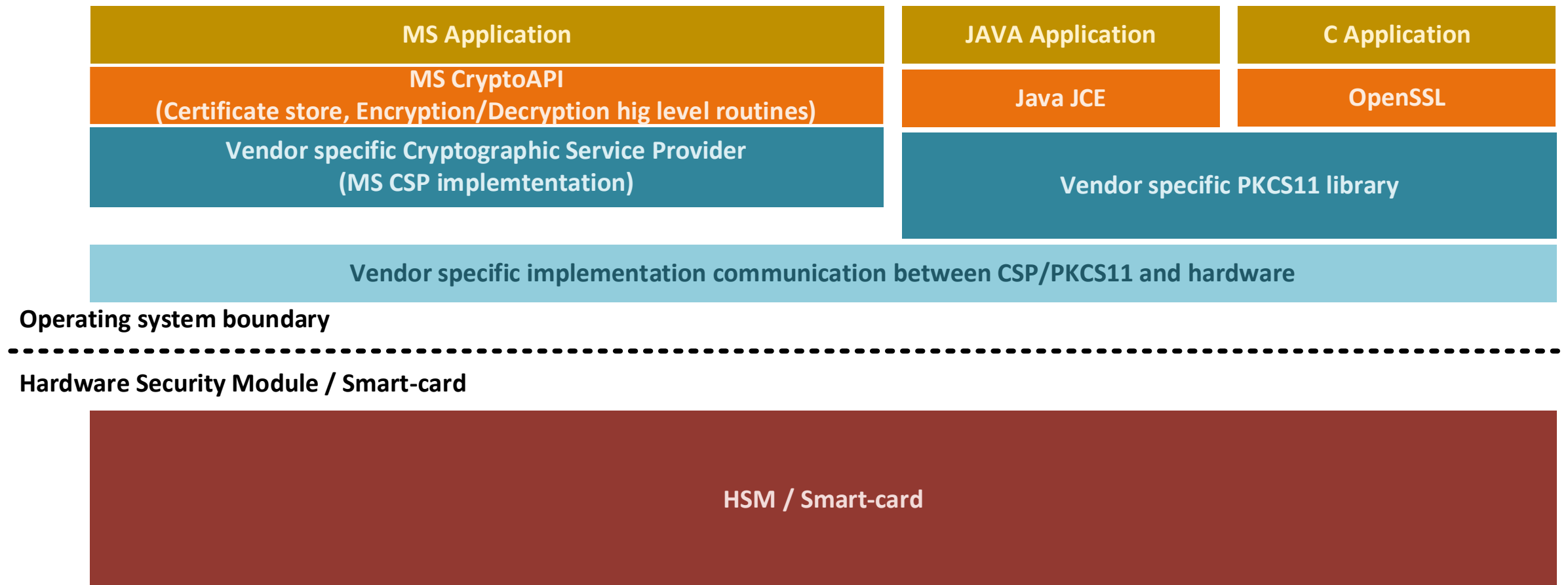
Uloženie a používanie kľúčov

Hardvérová ochrana kľúčov I.

- Posunutie / abstrakcia od uloženia kryptografických kľúčov priamo v systéme
- Využíva sa špecializovaný hardvér
 - Čipové karty
 - Trusted platform moduly / Secure element / Apple Secure Enclave / Samsung Secure Element
 - Hardvérové bezpečnostné moduly (HSM)
- Kryptografické kľúče nikdy neopúšťajú tento hardvér v nešifrovanom stave (nie je tým pádom možná ich krádež, **bez krádeže hardvéru**)
- Dedikovaný hardvér má obmedzený/znížený attack surface
- Zvyšok systému komunikuje so špecializovaným hardvérom prostredníctvom špecifického API
 - PKCS#11
 - CryptoAPI / CSP, CNG / KSP
 - ...

Uloženie a používanie kľúčov

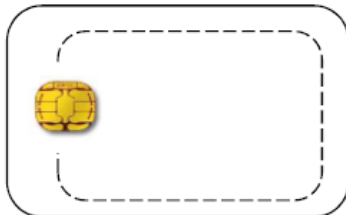
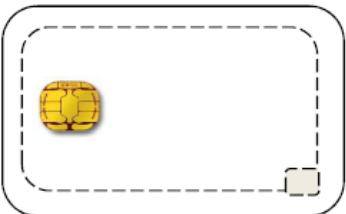
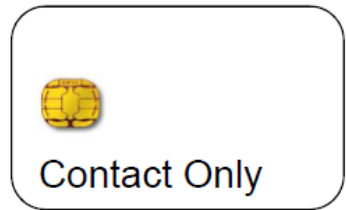
Hardvérová ochrana kľúčov I.



Uloženie a používanie kľúčov

Čipové karty I.

- Kontaktné
 - Běžné čipové karty v rozličných vyhotoveniach
 - Široké spektrum použitia: platobné karty, silná autentifikácia a šifrovanie, eID karty a pod.
- Bezkontaktné
 - Najčastejšie RFID
 - Používajú sa najmä na fyzické riadenie prístupu resp. pre jednoduchú identifikáciu osôb
- Hybridné
 - Kombinácia kontaktných a bezkontaktných
- Duálne
 - Kontaktný čip je prístupný cez anténu / bezkontaktné
 - Potrebná špeciálna čítačka pre bezkontaktné čítanie alebo podpora NFC v telefóne (Android)



Uloženie a používanie kľúčov

Čipové karty II – Windows Smart Card Stack

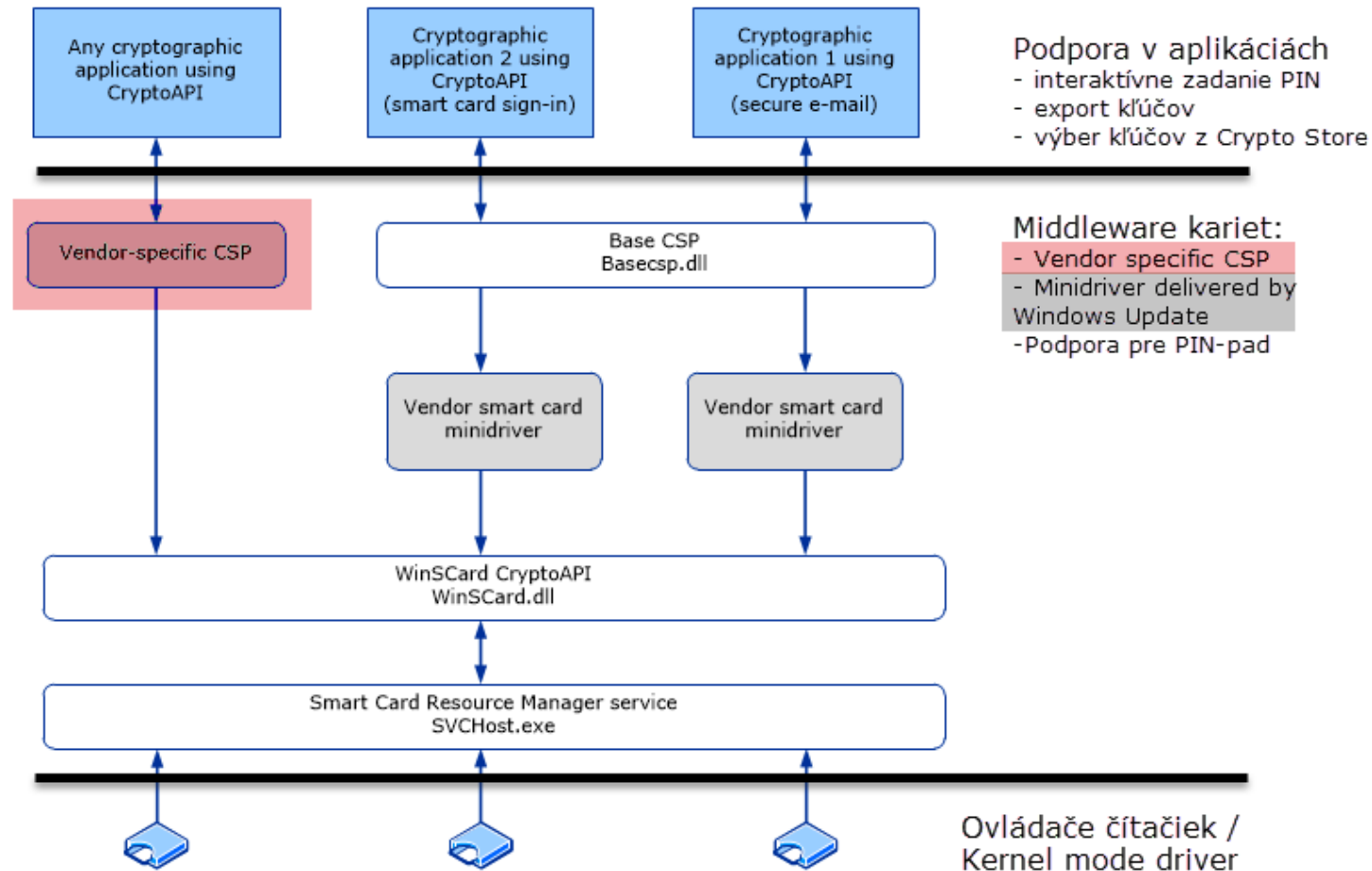
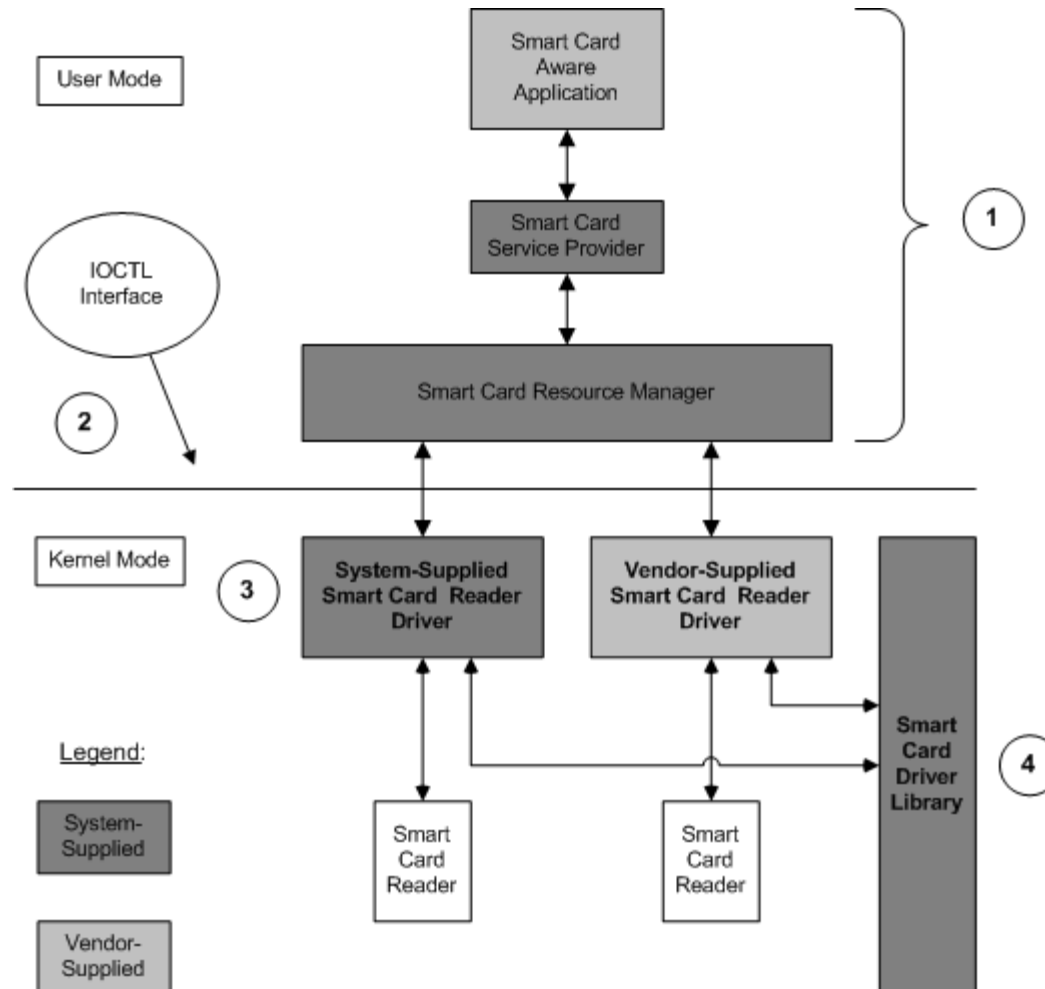


Figure 2 Base CSP and smart card minidriver architecture

Uloženie a používanie kľúčov

Čipové karty III – Windows Smart Card Stack



Uloženie a používanie kľúčov

Čipové karty IV.

- Aké sú výhody používania čipových kariet
 - Silná (dvojfaktorová) autentifikácia
 - Vyššia ochrana kryptografických kľúčov
 - Prenositelnosť kryptografických kľúčov, zbavenie sa duplikátov
- Aké sú problémy a nevýhody
 - Technické
 - Výber hardvéru, ovládačov, middleware (CSP/KSP@Windows, CDSA/Keychain@Mac, PKCS11, JCE/JCA), aplikácií a spolupráca/koexistencia kariet
 - Integrácia s mobilnými zariadeniami ([bluetooth reader](#) / duálne karty a NFC + [middleware](#) + špeciálne aplikácie pre email alebo browser)
 - Výkon (generovanie kľúčov / dešifrovanie / podpis), sériový prenos a blokovanie
 - Záloha kľúčov
 - Použitie kľúčov z webových aplikácií
 - Procesno-organizačné
 - Použitelnosť kariet
 - Zabudnuté karty
 - Blokované karty
 - Evidencia kariet (strata, ukončenie pracovného pomeru, permanentne blokované karty)
 - Cena nasadenia / údržby čipových kariet

Uloženie a používanie kľúčov

Čipové karty V.



Matthew Green ✓
@matthew_d_green



As a cryptographer I used to love chip cards. Then I had to use them. Down with the chips. Screw security.

[Preložiť Tweet](#)

2:54 AM · 4. 2. 2017 · Twitter for iPhone

39 retweetov **3** Tweety s citátom **159** označení Páči sa



Uloženie a používanie kľúčov

Trusted Platform Module

- Integrovaný čip „secure cryptoprocessor“
- Na rozdiel od čipových kariet majú štandardizované API
- Poskytuje
 - HW CS RNG
 - Bezpečné úložisko kryptografických kľúčov
 - Remote attestation (detekcia zmien v HW/SW) / secure boot
- Využíva sa často pri
 - Autentifikácii zariadení (napr. [conditional access](#))
 - Autentifikácii používateľa (tiež [conditional access](#))
 - Full-disk encryption
 - Ako náhrada čipových kariet
- Na rozdiel od čipových kariet je neprenositeľný a nedá sa použiť pre fyzický access control

Uloženie a používanie kľúčov

Secure Enclave / Secure Element

- Integrovaný čip „secure cryptoprocessor“ v mobilných zariadeniach de-facto TPM s drobnými odchýlkami
- Využíva sa často pri
 - Sprostredkovaní platieb
 - Full-disk encryption
 - Autentifikácii / secure boot
 - Bezpečné úložisko kryptografických kľúčov ale nie vždy využiteľné bežnými vývojarmi
- Obmedzený z pohľadu využitia bežnými vývojarmi
- Nie všetky mobilné zariadenia disponujú touto funkcionalitou, heterogénne prostredie

Uloženie a používanie kľúčov

Hardvérové šifrovacie moduly (Hardware Security Module)

- Na rozdiel od čipových kariet, TPM a secure enclave je HSM určený predovšetkým do serverového prostredia
- Má vyšší výkon a podporuje zálohu a obnovu kľúčov
- V minulosti bol výkon dokonca jednou z vlastností ktorá HSM pomáhala predávať, dnes môže byť výkon HSM skôr obmedzujúcou časťou riešenia
 - HSM môže mať limity počtu uložených/chránených kľúčov či už licenčné alebo dizajnové
 - HSM zväčša pracuje s kľúčmi v móde identifikácia / aktivácia / operácia, prvé dva kroky môžu chvíľu trvať preto ak výrobca povie že HSM zvládne 1 000 operácií s 2048 bit kľúčom za sekundu nemusí to nutne znamenať že s ľubovoľným kľúčom ale obyčajne s jedným a tým istým. S náhodným kľúčom to môže kludne byť aj 2/3 operácie za sekundu v závislosti od počtu kľúčov

Uloženie a používanie kľúčov

HSM

- V súčasnosti na trhu dvaja hráči
- Luna
 - Chrysalis/Rainbow (2003)
 - SafeNet 2004
 - Gemalto 2014
 - Thales 2019
- nShield
 - nCipher
 - Thales 2008
 - nCipher 2018
 - Entrust 2019
- Marvell LiquidSecurity HSM
- Ultimaco
- Ďalej sa venujeme nCipher nie kvôli kvalite ani trhovému podielu ale len z praktických príčin

Uloženie a používanie kľúčov

HSM – nCipher

nShield Solo

- PCIe karta / interný modul
- Prístupný len z jedného servera
- Nie je možné používať vo virtuálnych serveroch



nShield Connect

- Sieťové appliance / server
- Prístupný z viacerých serverov, je nevyhnutné spárovať klienta a HSM
- Možno využívať služby HSM aj z virtuálnych serverov



Uloženie a používanie kľúčov

Základný koncept nShield architektúry

- Kryptografické kľúče sú uložené v súboroch na **jednotlivých aplikačných serveroch**, ktoré ich využívajú v **šifrovanom stave** (šifrovaný pomocou kľúča ktorý pozná HSM)
- Ak aplikačný server chce využiť kľúč po prvý raz (za nejakú dobu) “nahrá” kľúč na HSM. HSM kľúč dešifruje (interne) a následne umožní pomocou neho vykonávať operácie dešifrovania / podpisovania
- Koncept takejto ochrany nazýva Thales/nCipher „**Security World**“

Uloženie a používanie kľúčov

nShield Security World

- Security World predstavuje de-facto bezpečnostnú hranicu
 - Security World vymedzuje kľúč, ktorý využíva HSM na dešifrovanie kľúčov od klientov
- Security World môže byť zdieľaný viacerými HSM
 - v rámci jedného Security World môže byť pripojených viacero HSM
 - Vhodné napr. pri potrebe zdieľať jeden kľúč medzi viacerými servermi (typický príklad pre vysoko-dostupné servery)
- Jedno HSM nemôže byť pripojené do viacerých Security World
- Jeden klient nemôže byť pripojený do viacerých Security World

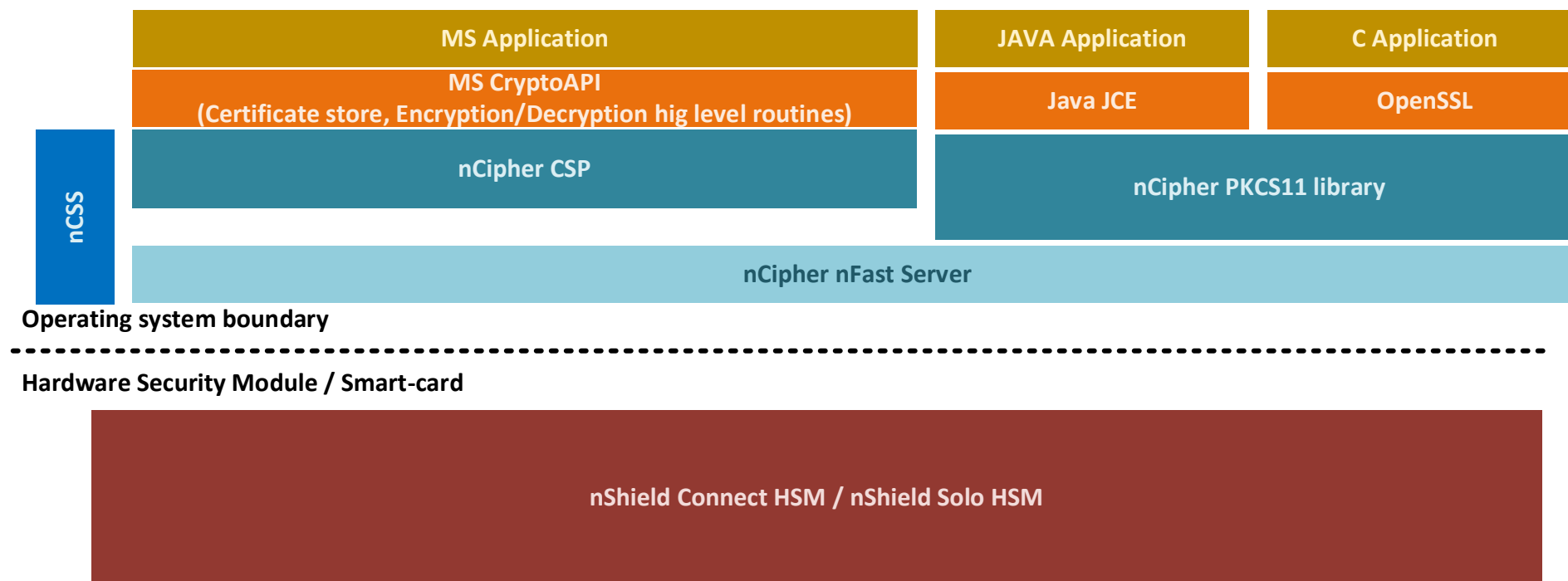
Uloženie a používanie kľúčov nShield Admin cardset

- Security World kľúč možno
 - Vygenerovať pri inicializácii HSM
 - Nahrať na HSM
- Inicializácia HSM / Generovanie Security World
 - Pri úvodnej konfigurácii HSM sa vygeneruje kľúč
 - Tento kľúč sa uloží do HSM a ako záloha sa rozdelí na niekoľko administrátorských kariet (Admin cardset) k/n schéma
 - Karty v rámci Admin cardset možno chrániť pomocou PINu
- Nahratie Security World na HSM
 - Potrebné vtedy ak sa HSM pripája do Security World (napr. kvôli vysokej dostupnosti alebo pri obnove HSM v prípade zlyhania)
 - Pri nahrávaní je nevyhnutné prezentovať **k z n administrátorských kariet** pre daný Security World

Uloženie a používanie kľúčov

nShield software stack

- Middleware nCipher Support Software (nCSSL)
 - Knižnice
 - nCipher CSP
 - nCipher KSP
 - PKCS11
 - Monitoring cez SNMP
 - Služba na komunikáciu s HSM (Windows Service / linux daemon)
 - Utility na správu a diagnostiku HSM



Uloženie a používanie kľúčov

nShield - Remote File System

- Súborový systém ktoré využívajú (sieťové) HSM na
 - Uloženie konfigurácie HSM (napr. informácie o klientoch)
 - Uloženie logov HSM
 - Na uloženie zašifrovaného kľúča Security World (možno použiť pri nahrávaní spolu s admin cardset)
 - Uloženie kľúčov v prípade, že sa používa RFS ako prostriedok pre ich zdieľanie medzi jednotlivými aplikačnými servermi
- Jeden HSM môže mať len jeden RFS server
- Jeden RFS server môže slúžiť pre viacero HSM

Uloženie a používanie kľúčov

nShield komunikačné toky

- V prípade PCIe / nShield Solo nie je nevyhnutné otvárať komunikačné toky (ak sa nepoužíva RFS na synchronizáciu kľúčov)
- V prípade nShield Connect (sieťové HSM) musí viesť:
 - aplikačný server komunikovať s ==> HSM (TCP:9004)
 - HSM komunikovať s RFS serverom (TCP:9004)
 - Každý klient je identifikovaný pomocou IP adresy a KNETI hash (niečo ako ekvivalent SSH hashu kľúča)
 - Nie je možné/prinajmenšom sa neodporúča mať medzi klientom a HSM NAT

Uloženie a používanie kľúčov

Hardvérové prostriedky sumár

- Nie je panacea a má svoje výhody a nevýhody
- V HSM, čipových kartách, TPM a pod. sa tiež našli chyby
 - ROCA
 - <https://cryptosense.com/blog/how-ledger-hacked-an-hsm>
 - <https://randomoracle.wordpress.com/2015/08/13/safenet-hsm-key-extraction-vulnerability-part-i/>
- Otázne výkonnostné charakteristiky
- Cena a správa
- Používateľská (ne)prívetivosť
- Supply chain
 - <https://www.schneier.com/blog/archives/2022/05/malware-infested-smart-card-reader.html>
- ...

Uloženie a používanie kľúčov

Cryptography as a service / Cloud Key Brokers 

- Služby ktoré umožňuje bezpečný spôsob uloženia, využitia a prístupu k certifikátom, privátnym kľúčom, heslám, API kľúčom a pod.
- Autentifikovaný prístup
- Príklady
 - Azure Key Vault
 - Hashicorp Vault
 - Amazon Web Service (AWS) Key Management Service (KMS)
- Výhody
 - Klasický trade-off služba tretej strany vs. in-house
- Nevýhody
 - V niektorých (najmä regulovaných) prostrediach problém so súladom s legislatívou / riešenie obyčajne BYOK (bring-your-own-key)
 - Ďalšia komplexita v systéme

Vd'aka