

česky



Modernisation of VET through  
Collaboration with the Industry

Ivan Pravda

Zabezpečení sítí



Erasmus+

Tento projekt byl realizován za finanční podpory Evropské unie.  
Za obsah publikací odpovídá výlučně autor. Publikace (sdělení) nereprezentují  
názory Evropské komise a Evropská komise neodpovídá za použití informací, jež  
jsou jejich obsahem.

**Název díla:** Zabezpečení sítí  
**Autor:** Ivan Pravda  
**Vydalo:** České vysoké učení technické v Praze  
Fakulta elektrotechnická  
**Kontaktní adresa:** Technická 2, Praha 6  
**Tel.:** +420 224352084  
**Tisk:** (pouze elektronicky)  
**Počet stran:** 40  
**Edice (vydání):** 1. vydání, 2019

**MoVET**

Modernisation of VET through  
Collaboration with the Industry

<https://movet.fel.cvut.cz>

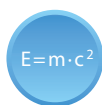


Tento projekt byl realizován za finanční podpory  
Evropské unie.

Za obsah publikací odpovídá výlučně autor.

Publikace (sdělení) nerepresentují názory Evropské  
komise a Evropská komise neodpovídá za použití  
informací, jež jsou jejich obsahem.

## VYSVĚTLIVKY



Definice



Zajímavost



Poznámka



Příklad



Shrnutí



Výhody



Nevýhody

---

## ANOTACE

Modul se zabývá možnostmi zabezpečení provozu sítí se zaměřením na oblast virtuálních privátních sítí (VPN). Definuje řadu základních pojmů, obsahuje popis základních komponent a konceptů sítí VPN. Dále je věnována pozornost vysvětlení protokolu IPSec a mechanismům umožňujícím implementaci zabezpečení provozu privátních sítí jakými jsou metoda ISAKMP/IKE a mechanismus výměny klíčů Diffie-Hellmann. Modul obsahuje v neposlední řadě i řadu praktických příkladů a jejich řešení. Závěr modulu je věnován problematice elektronického podpisu.

## CÍLE

Studiem modulu získají studenti přehled o problematice zabezpečení počítačových sítí prostřednictvím virtuálních privátních sítí. Tato problematika je dnes velmi aktuální, jelikož pojem bezpečnosti velmi úzce souvisí s kyberkriminalitou. Důraz je zde kladen nejen na objasnění terminologie v dané oblasti, ale i na vysvětlení principu základních postupů vhodně doplněnou o konkrétní příklady implementace. Závěrečná část objasňuje záležitosti týkající se elektronického podpisu a jeho možnosti implementace v každodenním životě.

## LITERATURA

- [1] Deal, Richard. The Complete Cisco VPN Configuration Guide. Cisco Press, 2005. 1032 pages. ISBN: 978-1-58705-204-0.
- [2] Cisco Systems. Clientless SSL VPN (WebVPN) on Cisco IOS with SDM Configuration Example. 2009. <https://www.cisco.com/c/en/us/support/docs/security/ssl-vpn-client/70663-webvpn.html> [online]
- [3] RFC4301 - Security Architecture for the Internet Protocol <http://tools.ietf.org/html/rfc4301> [online]
- [4] RFC4302 - IP Authentication Header <http://tools.ietf.org/html/rfc4302> [online]
- [5] RFC4303 - IP Encapsulating Security Payload (ESP) <http://tools.ietf.org/html/rfc4303> [online]
- [6] RFC4308 - Cryptographic Suites for IPsec <http://tools.ietf.org/html/rfc4308> [online]
- [7] RFC4364 - BGP/MPLS IP Virtual Private Networks (VPNs). <http://tools.ietf.org/html/rfc4364> [online]
- [8] RFC4835 - Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH) <http://tools.ietf.org/html/rfc4835> [online]

- [9] RFC5246 - The Transport Layer Security (TLS) Protocol Version 1.2.  
<http://tools.ietf.org/html/rfc5246> [online]

# Obsah

<b>1</b>	<b>Virtuální privátní síť – definice základních pojmů .....</b>	<b>7</b>
<b>2</b>	<b>Komponenty VPN .....</b>	<b>9</b>
<b>3</b>	<b>Rozdělení VPN dle RM-OSI.....</b>	<b>11</b>
<b>4</b>	<b>Protokol IPSec – popis .....</b>	<b>13</b>
<b>5</b>	<b>Výměna klíčů u protokolu IPSec – metoda ISAKMP/IKE .....</b>	<b>16</b>
<b>6</b>	<b>Algoritmus Diffie-Hellmann.....</b>	<b>20</b>
<b>7</b>	<b>Útoky v lokálních sítích – příklady a řešení.....</b>	<b>22</b>
<b>8</b>	<b>Budování VPN pomocí IPSec – příklady a řešení.....</b>	<b>26</b>
	8.1 Příklad konfigurace IPSec VPN na zařízeních fy.Cisco .....	29
<b>9</b>	<b>Budování VPN pomocí SSL/TLS – příklady a řešení.....</b>	<b>31</b>
	9.1 Typy přístupů SSL VPN.....	32
<b>10</b>	<b>Elektronický podpis .....</b>	<b>34</b>
	10.1 Zaručený elektronický podpis .....	36
	10.2 Kvalifikovaný elektronický podpis .....	38
	10.3 Elektronická pečeť.....	39
	10.4 Časové razítko .....	40

# 1 Virtuální privátní síť – definice základních pojmů

$E=m \cdot c^2$

## FORMÁLNÍ DEFINICE

Virtuální privátní síť **VPN** (*Virtual Private Network*) je komunikační prostředí, ve kterém je řízen přístup ke komunikaci mezi jednotlivými entitami. Komunikační prostředí je vytvořeno na bázi předem definované formy rozdělení společného komunikačního média, které je následně schopno poskytovat síťové služby na ne-exkluzivní bázi.

$E=m \cdot c^2$

## NEFORMÁLNÍ DEFINICE

Virtuální privátní síť **VPN** je neveřejná (počítačová) síť, vybudovaná v rámci veřejné síťové infrastruktury, jakou je např. Internet. Tato síť typicky zajišťuje zabezpečené připojení vzdálených poboček nebo účastníků k mateřské síti.



Z předchozích definic lze stručně říci, že VPN je ve své podstatě logická síť v rámci sdílené veřejné infrastruktury. Poskytuje stejný výkon a pravidla jako kterákoliv soukromá síť typu **LAN** (*Local Area Network*).

Zcela zásadním problémem při použití VPN je zajištění její bezpečnosti a poskytování služeb v požadované kvalitě s ohledem na ukazatele **QoS** (*Quality of Service*). Oba tyto požadavky neřeší infrastruktura sítě založená na protokolech **TCP/IP** (*Transmission Control Protocol/Internet Protocol*).

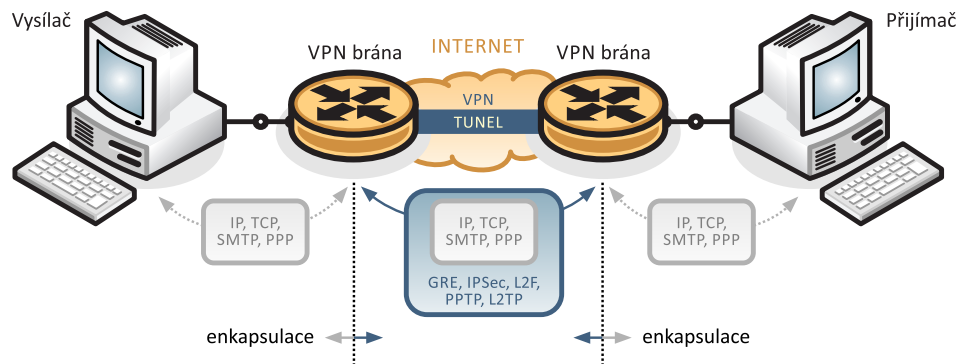
Požadavky na bezpečnost se z hlediska návrhu VPN řeší pomocí:

- tunelování,
- šifrování,
- autentizace a
- řízení přístupu.

$E=m \cdot c^2$

Pojmem tunelování je chápán proces zapouzdření původního paketu do jiného. Původní paket je pro všechna mezilehlá zařízení nečitelný po celou dobu jeho přenosu.

Důvodem pro implementaci tunelování je zajištění bezpečnosti a vytvoření transportního mechanismu mezi geograficky odlehlými lokalitami. K zapouzdření se používají např. protokoly **GRE** (*Generic Routing Encapsulation*), **IPSec** (*Internet Protocol Security*), **L2F** (*Layer 2 Forwarding*), **PPTP** (*Point-to-Point Tunneling Protocol*), **L2TP** (*Layer 2 Tunneling Protocol*).



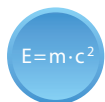
Mechanismus tunelování v síti VPN



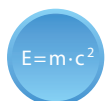
Tunelování je ovšem možné využít také pro přizpůsobení navzájem nekompatibilních protokolů, např. propojení LAN s **NetBEUI** (*NetBIOS Extended User Interface*) nebo **IPX** (*Internetwork Packet Exchange*) přes Internet (protokol IP).



Reálně je možné implementovat i tzv. rozdělené tunelování (Split Tunneling), kdy má klient možnost současné komunikace jak uvnitř VPN, tak i s Internetem.



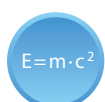
Pod pojmem šifrování rozumíme proces pro zajištění důvěrnosti i integrity dat. Čistě technicky jde o zapouzdření dat do bezpečné obálky, tj. šifrování tajným klíčem.



Autentizace v rámci VPN zajišťuje proces ověřování pravosti, resp. zabezpečí, že data přicházejí ze zdroje, ze kterého tvrdí, že přicházejí.



Používají se schémata založená na systémech se sdíleným klíčem, jako je **CHAP** (*Challenge Handshake Authentication Protocol*), signatura **RSA** (*Rivest–Shamir–Adleman*) a další. Nad rámec zabezpečení zajišťují tyto systémy také integritu dat, tj. jejich celistvost.



Řízení přístupu, resp. kontrola přístupu umožňuje omezování přístupu či vniknutí neautorizovaných uživatelů ve spojitosti s procesem kontroly práv jednotlivých uživatelů.



## 2 Komponenty VPN

Sítě VPN používají k zabezpečení šifrovací tunelovací protokoly a poskytují ochranu proti odposlechu paketů (Packet Sniffing), zaručují odpovídající autentizaci a deklarují úplnost zpráv, tj. jejich integritu.



---

Komponenty nezbytné k vybudování VPN spojení jsou:

- existující síť typu LAN nebo samostatný terminál (např. PC, notebook, netbook, apod.),
- dostupné připojení k Internetu,
- VPN brány, tzv. VPN Gateways (např.: směrovače, firewally, VPN koncentrátoři) a
- odpovídající programové vybavení (Software) potřebné k budování a spravování VPN tunelů.

---

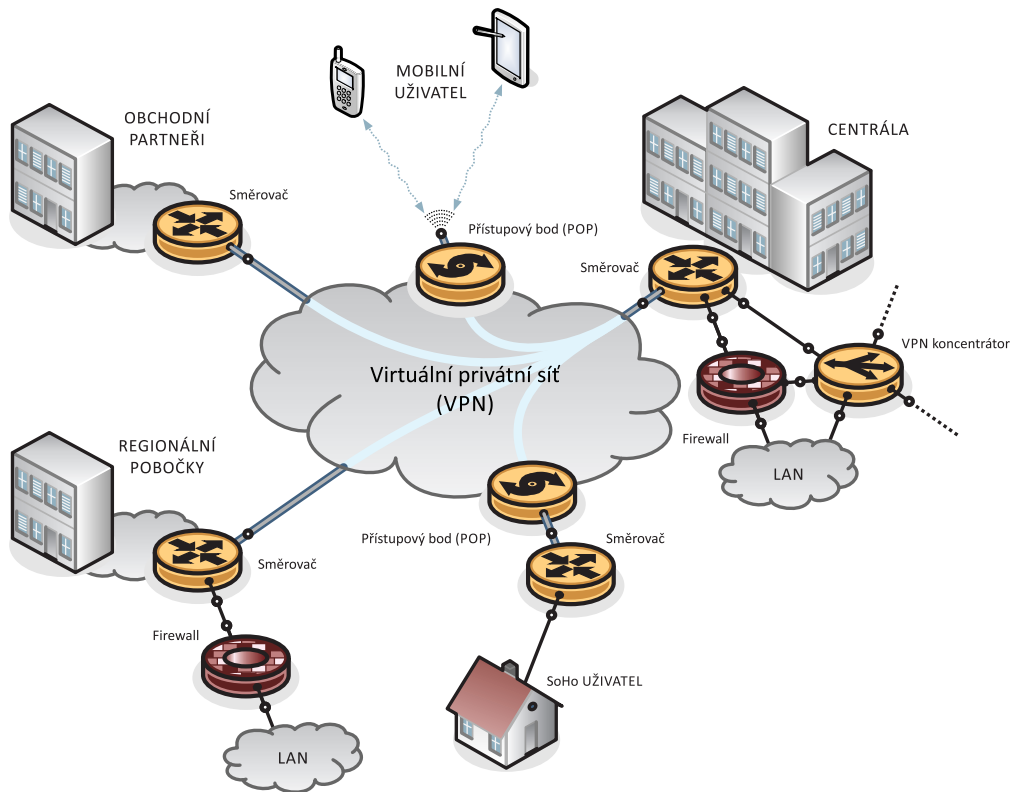
### 1. Spojení síť-síť (Site-to-Site nebo LAN-to-LAN)

Tento typ spojení sítí přes VPN je využíván k propojení geograficky rozptýlených míst obdobným způsobem, jako kdyby byly tyto lokality propojeny pronajatou linkou nebo jinou WAN (*Wide Area Network*) technologií (např. Frame-Relay, ATM (*Asynchronous Transfer Mode*)). Výhodou takového propojení je sdílení podnikového intranetu nebo extranetu s pracovním partnerem. V této topologii, uživatelé posílají a přijímají data prostřednictvím VPN brány, kterou bývá obvykle směrovač nebo server. VPN brána je zodpovědná za šifrování odchozího provozu a jeho směrování do VPN tunelu v Internetu k protější VPN bráně cílové sítě. Tato VPN brána odebere hlavičku paketu, dešifruje jeho obsah a následně doručí paket k cílovému uživateli uvnitř cílové sítě.

### 2. Spojení typu vzdálený přístup (Remote-Access)

Terénní pracovníci či domácí pracovníci využívají vzdálený přístup VPN připojením velmi hojně. V minulosti byli tito vzdálení pracovníci připojováni telefonními linkami, což znamenalo nízkou rychlost přenosu spojenou s vysokými náklady na provoz. V současnosti však již většina z nich disponuje rychlým přístupem k internetu přímo z domova prostřednictvím širokopásmových technologií a mohou tak vybudovat kvalitní VPN spojení.

Každý uživatel má typicky nainstalovaný VPN klient, tj. software, který zapouzdřuje a šifruje pakety před tím, než je odešle přes Internet k cílové VPN bráně. Tento software tak významně usnadňuje připojení, jelikož uživateli stačí pouze základní znalosti k vybudování kvalitního VPN spojení.



Možnosti propojení pomocí VPN

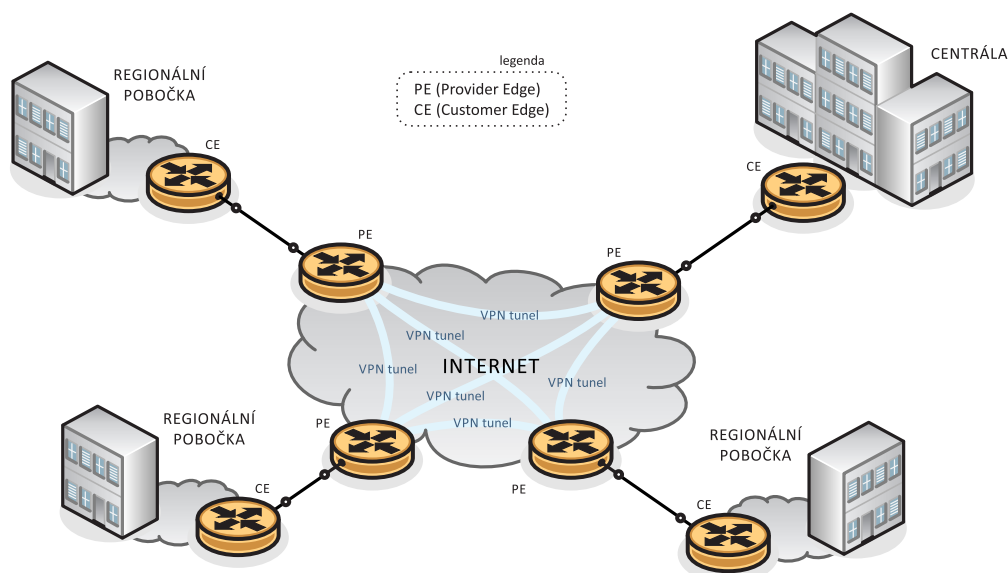
### 3 Rozdělení VPN dle RM-OSI

#### 1. VPN založené na zařízení provozovatele (PE-based VPN)

$E=m \cdot c^2$

Zařízení **PE** (*Provider Edge*) je hraniční zařízení poskytovatele připojení a řadíme mezi ně směrovače **ISP** (*Internet Service Provider*), přepínače nebo zařízení, která jsou kombinací obou.

Zařízení typu PE se účastní směrování a přeposílání provozu na základě adresního prostoru zákazníka. Data jsou obvykle přenášena mezi zařízeními PE prostřednictvím VPN tunelů vytvořených pomocí technologie **MPLS** (*Multi Protocol Layer Switching*), IPsec, L2TPv3 nebo GRE. V tomto případě zařízení **CE** (*Customer Edge*) nevnímají, že jsou součástí VPN.



Uspořádání VPN založené na zařízení provozovatele

*i*

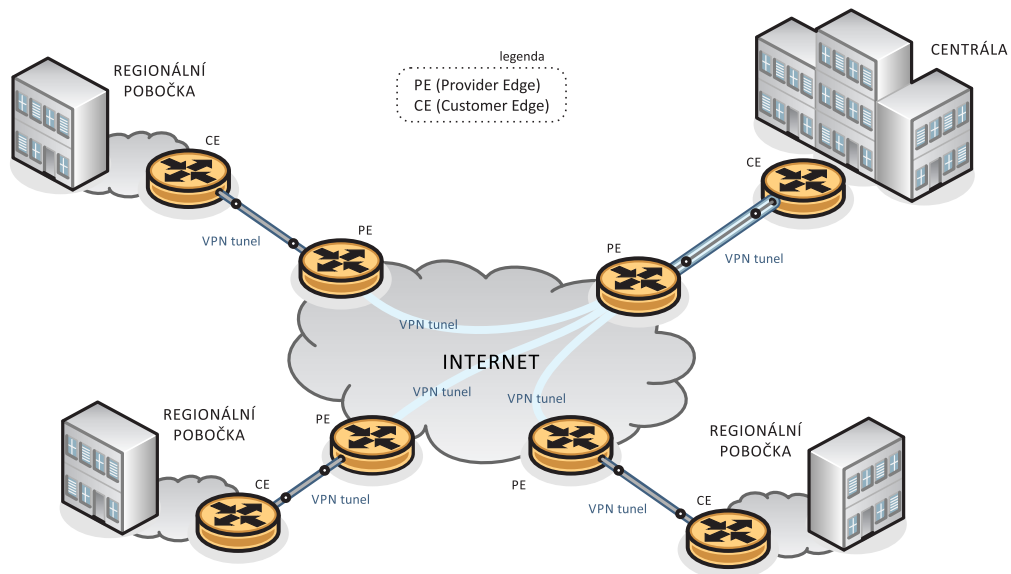
VPN tunely jsou ukončeny na hraničním směrovači PE a jsou obvykle konfigurovány jako permanentní.

#### 2. VPN založené na zařízení zákazníka (CE-based VPN)

$E=m \cdot c^2$

Zařízení **CE** je hraniční zařízení zákazníka propojené se zařízením provozovatele PE.

Zařízení PE v tomto módu nerozlišují typ provozu, o VPN spojení se starají zařízení CE, která provádí směrování a posílání provozu uživatele. Tunely jsou vytvořeny mezi zařízeními CE na základě protokolů IPsec nebo GRE.



Uspořádání VPN založené na zařízení zákazníka



Zařízení CE (VPN brána) většinou plní i další funkce pro VPN klienty (např. server **DHCP** (*Dynamic Host Configuration Protocol*), doménový server **DNS** (*Domain Name Server*)). Toto řešení obecně klade vyšší nároky na autentizaci klientů, jelikož se připojují kdykoliv a odkudkoliv.

## 4 Protokol IPSec – popis

$E=m \cdot c^2$

Protokol IPSec je komplexním souborem protokolů řešící šifrování, autentizaci, integritu dat a proces tunelování. Zabezpečení je realizováno na síťové vrstvě referenčního modelu **OSI** (*Open System Interconnection*), a proto poskytuje transparentně bezpečnost jakémukoliv přenosu, resp. libovolné síťové aplikaci.

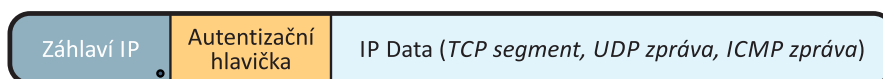
Mezi základní komponenty protokolu IPSec patří:

- bezpečnostní protokoly – **AH** (*Authentication Header*), **ESP** (*Encapsulating Security Payload*),
- protokoly pro výměnu klíčů – **ISAKMP** (*Internet Security Association and Key Management Protocol*), **IKE** (*Internet Key Exchange*),
- pomocné databáze – **SPD** (*Security Policy Database*), **SAD** (*Security Association Database*) a
- **DOI** (*Domain Of Interpretation*) – obsahuje různé hodnoty jako např. identifikátory a ukazatele pro **SA** (*Security Association*)

Protokol IPSec umožňuje dva pracovní režimy:

1. transportní režim – určený pro spojení typu Host-to-Host

V transportním režimu je obvykle zašifrován nebo ověřen pouze obsah daného IP paketu. Směrovací informace zůstává nezměněna, pokud není hlavička IP paketu upravena ani šifrována. Při použití autentizační hlavičky **AH** (*Authentication Header*) nemohou být IP adresy přeloženy, jelikož se vždy ztratí právo na hodnotu hash. Transportní a aplikační vrstvy jsou vždy zabezpečeny hashovací funkcí, takže nemohou být nijak upravovány (např. změnou čísla portu).

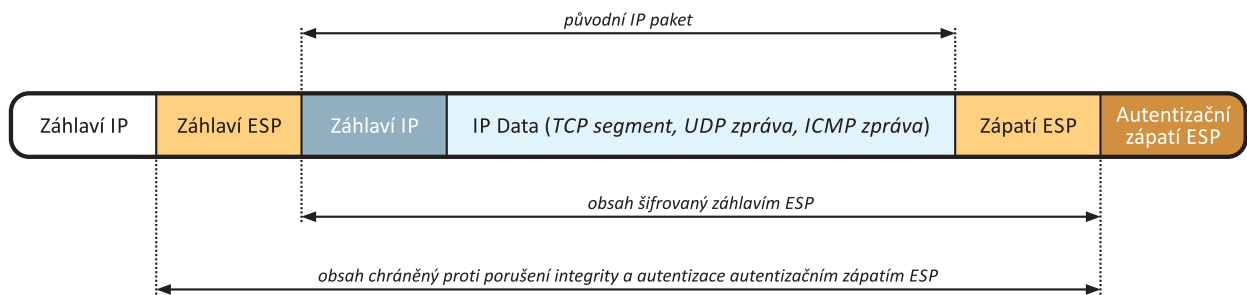


IP hlavička zůstává stejná kromě změny indikace, že jde o IPSec protokol

Struktura paketu IPSec v transportním režimu s využitím hlavičky AH

2. tunelovací režim – určený primárně pro spojení typu Site-to-Site

V tunelovacím režimu je šifrován nebo ověřován celý IP paket pomocí **ESP** (*Encapsulating Security Payload*). Následně je zapouzdřen do nového IP paketu se zcela novou hlavičkou využitím autentizační hlavičky **AH**. Tento režim se používá pro tvorbu sítí VPN určených pro komunikaci mezi jednotlivými sítěmi Site-to-Site (např. mezi směrovači propojující různé sítě), Host-to-Site komunikaci (např. vzdálený přístup uživatele) a Host-to-Host komunikaci (např. soukromý chat).



Struktura paketu IPsec v tunelovacím režimu s využitím ESP



Tunelovací režim tunelu podporuje **NAT** (*Network Address Translation*) a **PAT** (*Port Address Translation*).



Protokol IPsec neobsahuje v záhlaví žádné pole určující typ režimu. Pracovní režim je nastaven dle hodnoty pole Next Header (hodnota „IP“ specifikuje tunelovací režim, hodnoty „TCP, UDP, ICMP“ nebo cokoliv jiného identifikují transportní režim).



Mezi výhody protokolu IPsec patří jeho transparentnost, tzn. není potřeba nijak modifikovat protokoly vyšších vrstev, protokol IPsec může zabezpečit libovolný protokol využívající protokol IP, zabezpečuje i „staré“ protokoly, které jsou nezabezpečené a je široce podporován výrobci **HW** (*Hardware*) a **SW** (*Software*).



K nevýhodám protokolu IPsec patří zvýšení systémové režie (*overhead*), nutnost instalace klienta v případě vzdáleného přístupu, sám o sobě neřeší autentizaci uživatele, komplikace s NAT a PAT (možný pouze v tunelovacím režimu) a s přenosem provozu typu multicast a broadcast.



Protokol IPsec:

- zabezpečuje provoz na síťové vrstvě,
- je univerzální pro zabezpečení libovolného TCP/IP provozu,
- chrání před analýzou provozu na úrovni síťové vrstvy tzv. Packet Sniffing,
- je vhodný pro pevné připojení vzdálených uživatelů,
- nepodporuje přenos multicast a broadcast,
- má problémy s překladem adres (NAT a PAT) – mění se adresní pole chráněná **HMAC-SHA1** (*Hash Message Authentication Code - Secure Hash Algorithm*),

řešením je zabalit IPSec paket do datagramu **UDP** (*User Datagram Protocol*)  
→ metoda **NAT-T** (*NAT-Traversal*) a

- v případě vzdáleného přístupu je vyžadována instalace klienta (mohou však vzniknout problémy s kompatibilitou různých implementací).
-

## 5 Výměna klíčů u protokolu IPSec – metoda ISAKMP/IKE

Výměna klíčů mezi klienty před započítím vlastní zabezpečené komunikace je důležitá hned z několika hledisek. Vystává zde však otázka, jak vlastně řešit bezpečnou výměnu klíčů? Před vlastní komunikací je nutné zajistit:

1. dohodu na typu klíče a způsobu jeho tvorby, tj. stanovit sdílený klíč **PSK** (*Pre-Shared Key*)
2. autentizaci účastníků, tj. vzájemné ověření identity účastníků komunikace
3. ochranu identity účastníků, tj. pasivní útočník nemá být schopen odhalit identitu účastníků pouhým sledováním komunikace
4. ochranu proti **DoS** (*Denial of Service*), tj. zlomyslný uživatel by neměl být schopen zneužít protokol tak, aby nutil protistranu plýtvat zdroji (**CPU** (*Central Processing Unit*), paměť, kapacita úložiště, ...)

$E=m \cdot c^2$

Protokol ISAKMP je definován doporučením RFC 2408. Pro svou činnost využívá transportní protokol UDP na portu 500.



Protokol ISAKMP je obecným protokolem pro vytváření SA, tj. neřeší, jak konkrétně se mají autentizované klíče vyměnit. To je práce protokolu IKE. Protokol ISAKMP slouží k autentizaci komunikujících stran a výměně dat pro šifrovací klíče.

*i*

Nejedná se o komunikaci typu Klient-Server, ale typu Výzva-Odpověď. Strana, která chce vytvořit nové SA iniciuje komunikaci protokolem ISAKMP.

$E=m \cdot c^2$

Protokol IKE je flexibilní vyjednávací protokol definovaný doporučením RFC 2409. Umožňuje vyjednání konkrétní metody autentizace, šifrování, délek klíčů a jejich bezpečnou výměnu. Pro svou činnost používá Diffie-Hellmanův algoritmus (D-H algoritmus).

*i*

Protokol IKE je využíván k výměně relačních klíčů, tzv. Session Keys. Zprávy protokolu IKE jsou zapouzdřeny do paketů protokolu ISAKMP.

Činnost protokolu IKE lze rozdělit na dvě nezávislé fáze. První fáze realizuje sestavení bezpečného autentizovaného kanálu mezi komunikujícími entitami (počítači). V rámci této fáze je chráněným způsobem autentizována identita komunikujících stran. Obě komunikující strany se dohodnou, jaké použijí SA



a provedou autentizovanou výměnu sdílených klíčů PSK. Následně je sestaven bezpečný tunel pro druhou fázi. Pro sestavení tunelu jsou k dispozici dva režimy:

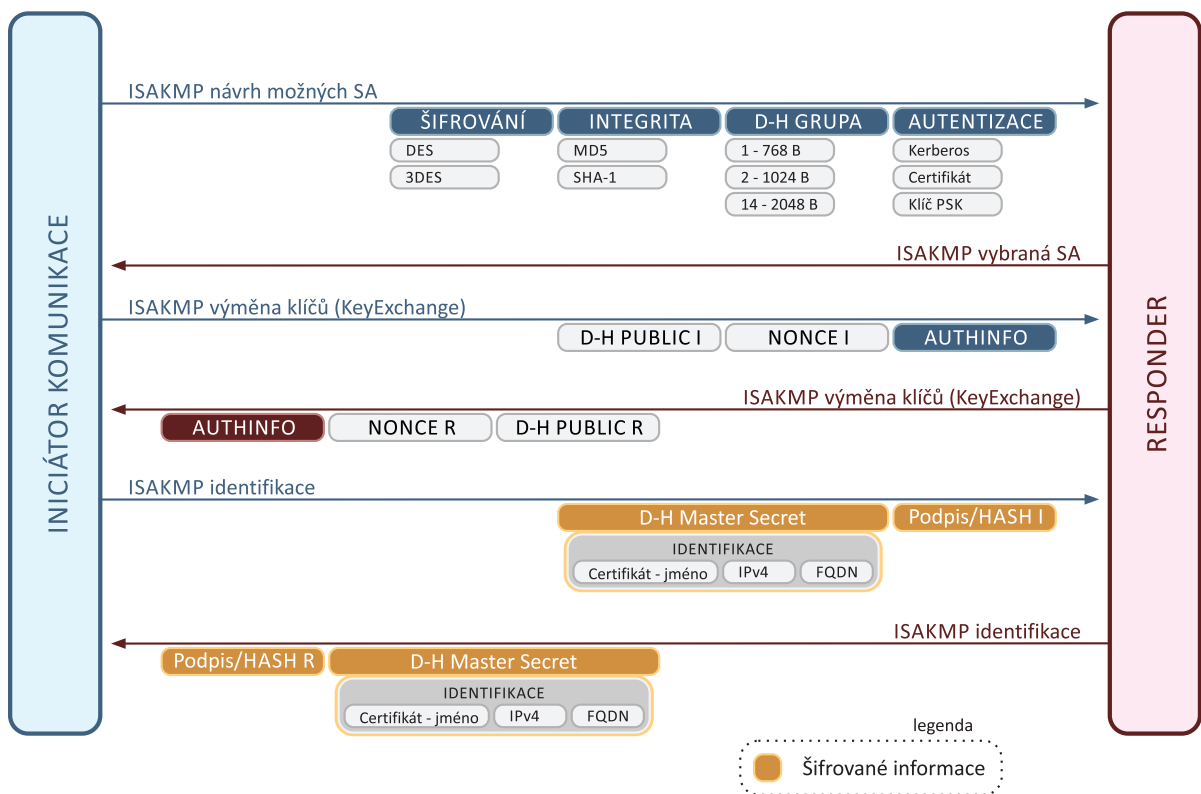
- hlavní režim, tzv. Main Mode
  - dojedná algoritmy a hashovací funkce, vygeneruje sdílené tajemství pomocí D-H algoritmu a ověří identitu protistrany. Celkem jde o 6 zpráv
- agresivní režim, tzv. Aggressive Mode
  - zkrátí vyjednávání do menšího množství paketů. Celkem jde o 3 zprávy.



Výhodou agresivního režimu je úspora přenosového pásma a času nutných pro přenos zpráv.



Nevýhodou agresivního režimu je výměna důležitých informací ještě před sestavením šifrovaného spojení, což je náchylné na odposlech, tzv. Sniffing.



Procesní diagram Fáze 1 protokolu IKE (hlavní režim)



V první fázi je možné využít čtyř různých způsobů výměny klíče PSK:

- asymetrické šifrování veřejným klíčem (původní verze)

- asymetrické šifrování veřejným klíčem (zdokonalená verze)
  - digitální podpis
  - tajný klíč (dle symetrického algoritmu)
- 



Každou variantu výměny klíče lze využít v hlavním nebo agresivním režimu, tj. dohromady existuje osm různých variant první fáze protokolu IKE !!! Hlavní režim musí být implementován vždy, agresivní režim je volitelný, tj. měl by být implementován.

---



Výsledkem první fáze protokolu IKE je vzájemná autentizace komunikujících stran, výměna sdíleného symetrického klíče PSK a ustanovení IKE Security Association (SA).

---

Druhá fáze (tzv. Quick Mode) vytvoří SA pro IPSec relaci, tj. dojednávají se parametry SA IPsec spojení, dochází k sestavení IPsec SA pro konkrétní spojení (např.: FTP, telnet, apod.), provádí se periodická obnova IPsec SA, volitelně jsou realizovány další D-H výměny a specifikuje se další klíčový materiál pro vlastní komunikaci.

---



Tato komunikace je od počátku chráněna pomocí algoritmů a klíčů získaných během první fáze.

---

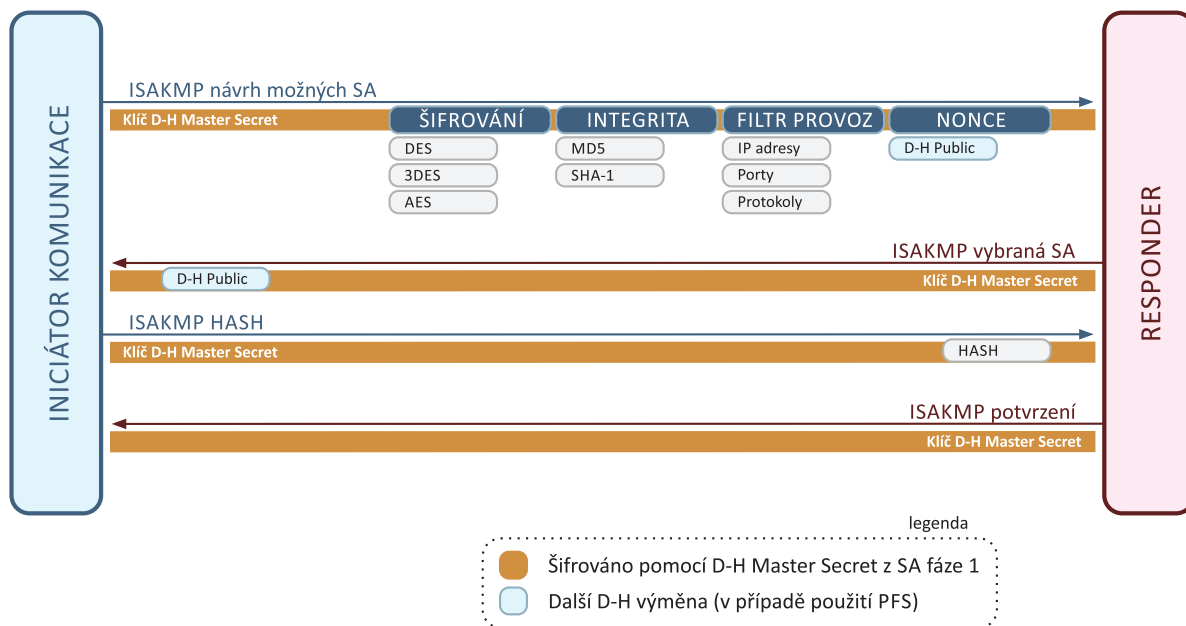
Pro šifrování běžné komunikace se použije relační klíč (Session Key) odvozený z D-H Master Key získaného z Main Mode SA a z Nonce dané Quick Mode SA.

---



Využití **PFS** (*Perfect Forward Secrecy*) označuje stav, kdy nejsou aktuální klíče použity ke generování dalších klíčů. Je-li totiž náhodou konkrétní klíč rozšifrován, tj. prozrazen, neumožní to útočníkovi snadné rozlomení dalších klíčů. Pokud je PFS použito, pak se v Quick módu znovu generuje pomocí D-H nová sdílená tajná informace. Využití PFS je bezpečnější, ale trochu náročnější na výkon a čas při sestavování spojení. Relační klíč se získá z nového D-H Secret Key a Nonce získaných z dané Quick Mode SA. Aplikací PFS je tak zajištěno, že relační klíč není nikdy generován ze stejného materiálu.

---



Procesní diagram Fáze 2 protokolu IKE (Quick Mode)



Porovnání se SSL/TLS – SSL relace odpovídá první fázi činnosti protokolu IKE, SSL spojení odpovídá druhé fázi činnosti protokolu IKE.

## 6 Algoritmus Diffie-Hellmann

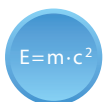
Diffie-Hellmanův algoritmus (D-H algoritmus) je kryptografický protokol, který umožňuje vytvořit mezi komunikujícími stranami šifrované spojení přes nezabezpečený kanál, a to bez nutnosti dopředu dohodnout šifrovací klíč. Výsledkem algoritmu je symetrický šifrovací klíč, který může být následně použit pro šifrování zbytku komunikace.



Výhodou je, že případný útočník odposlouchávající komunikaci tento klíč nezachytí. Klíč je totiž vytvořen všemi účastníky komunikace a nikdy není poslán v otevřené formě. Resp. tento algoritmus zaručí výměnu společného klíče takovým způsobem, že pokud tuto komunikaci odposlouchává útočník, pak není schopen společný klíč na základě odposlechnutých informací zrekonstruovat.



Nevýhodou tohoto protokolu je bezbrannost proti útoku Man in the Middle, protože neumožňuje autentizaci účastníků. Tento protokol bez kombinace s jinými metodami autentizace je tedy vhodný pouze tam, kde útočník nemůže aktivně zasahovat do vlastní komunikace.



Princip D-H algoritmu definovaný doporučeními RFC 2409, RFC 3526 a RFC 5114 je založen na umocňování čísel  $(A^B)^C = (A^C)^B$ , resp. na modulární variantě tohoto vzorce  $(A^B)^C \bmod m = (A^C)^B \bmod m$ .

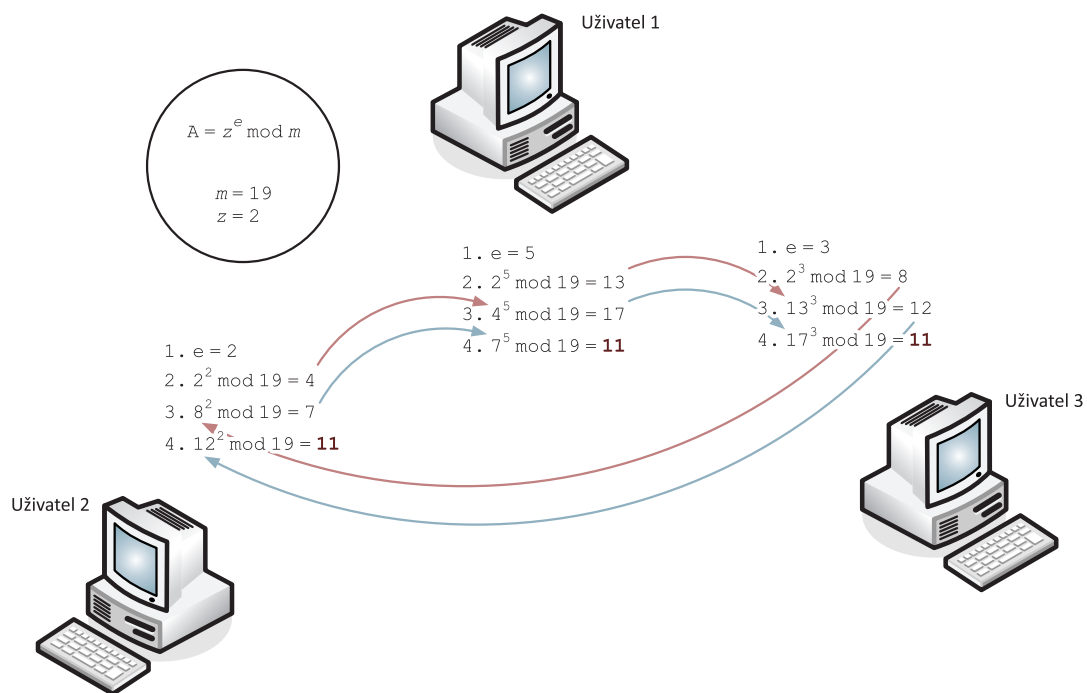


Velikost modulu pak specifikuje typ grupy. Obvykle se používají grupy 1, 2 a 5. Číslo grupy udává délku klíče – DH-1 (768 bitů), DH-2 (1024 bitů), DH-5 (1535 bitů), DH-14 (2048 bitů).

Výpočet výsledné hodnoty je velmi snadný (rychlý), ale jen velmi obtížně se dá zjistit některá z hodnot, kterou zná pouze jiný účastník. Tomuto principu, na kterém stojí bezpečnost tohoto algoritmu, se říká problém diskretního logaritmu.

Komunikace s využitím D-H algoritmu probíhá následujícím způsobem:

- Účastníci se veřejně domluví na použitém modulu  $m$ , resp. typu grupy a základu  $z$ .
- Každý z účastníků si zvolí svůj exponent  $e$  (nesoudělný s modulem  $m$ ).
- Každý z účastníků umocní modulárně základ na svůj exponent a výsledek pošle dalšímu účastníkovi.
- Algoritmus končí, když je každý z původních základů zpracován každým účastníkem.



Princip komunikace tří účastníků pomocí Diffie-Hellmanova algoritmu

## 7 Útoky v lokálních sítích – příklady a řešení

Bezpečnost síťových prvků byla velmi dlouho podceňována a firmami odsouvána do pozadí. V poslední době se ovšem trend mění a řada podniků si uvědomuje význam a důsledky potenciálních hrozeb. Počet útoků zevnitř sítě rapidně převažuje počet útoků zvenku sítě. Proto se budeme zabývat zabezpečením přístupových přepínačů (Access Switch), ke kterým mají uživatelé přímý přístup, a kde tak vzniká vysoké potenciální riziko různých typů útoků.

Příklady možných útoků na přepínače:

- MAC-Address Flooding – přeplnění tabulky CAM (*Content Addressable Memory*) → přepínač se pak chová jako obyčejný rozbočovač (HUB)
- DHCP Spoofing – podvržení DHCP adresy útočným DHCP serverem
- zneužití Trunk portu – útočník má poté přístup k provozu z dalších přenášených VLAN (*Virtual LAN*)
- útoky prostřednictvím zpráv CDP (*Cisco Discovery Protocol*) – zprávy protokolu CDP nejsou šifrovány, odesílají se periodicky a poskytují detailní informace o typu zařízení, verzi IOS atd.
- další útoky – např. útoky na hesla vzdáleného přístupu, DoS útoky, apod.
- instalace neautorizovaných bezdrátových přístupových bodů (Rogue AP), které si zaměstnanec nainstaluje, aby měl na pracovišti např. dostupný Internet pro své PDA (*Portable Digital Assistant*), a který tak kvůli svému nedostatečnému zabezpečení může zpřístupnit vnitřní síť firmy...

Možná řešení:

### 1. Port Security



---

Port Security je nejjednodušší způsob zabezpečení portů, které slouží ke kontrole adres MAC (*Medium Access Control*) připojených na daných port. V případě porušení definovaného pravidla se provede akce podle toho, jak byl port nastaven.

---

Existují tři reakce na narušení bezpečnosti:

- Protect - povolené MAC adresy mohou nadále komunikovat, komunikace z nepovolených MAC adres je zablokována
- Restrict – chování je stejné jako v režimu Protect, ale navíc se vygeneruje chybové hlášení do logu zařízení a pokud je nakonfigurováno SNMP (*Simple Network Management Protocol*), odešle se SNMP trap na SNMP server
- Shutdown – veškerá komunikace (i z povolených adres) je zablokována. Port je přepnut do speciálního stavu Error-Disable, kdy je nutný zásah správce a opětovné manuální zapnutí portu.



---

Takto nastaveným způsobem zabezpečení provážíme daný fyzický port s pevně přidělenou virtuální sítí (VLAN). Tím vznikne pevná vazba skupiny MAC adres a jedné VLAN na daný přístupový port.

---



Pro rozsáhlé podnikové sítě není předchozí řešení dostačující a používají se komplexní integrovaná řešení jako je např. řešení založené na protokolu (doporučení) IEEE 802.1X.

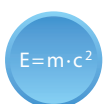
---

Zabezpečení Port Security se na Cisco přepínači provede následovně. Nejprve je třeba na zvoleném portu zapnout funkci Port-Security pomocí příkazu „switchport port-security“. Výchozí hodnota je 1, což znamená, že k danému portu lze připojit pouze jedno zařízení. Tuto hodnotu, tj. povolený počet MAC adres, které mohou na daný port přistupovat, lze změnit. Adresy se přepínač také může učit buď dynamicky, nebo je lze nastavit ručně. Ruční nastavení se realizuje pomocí příkazu „switchport port-security mac-address MAC-ADRESA“. Tento příkaz lze rozšířit parametrem „sticky“, který zajistí, aby se dynamicky naučená MAC adresa uložila do konfigurace zařízení. Jak bylo uvedeno dříve, nyní je třeba nastavit akci, kterou přepínač provede v případě porušení pravidel pomocí příkazu „switchport port-security violation“. Vše je názorně vidět na následujícím výpisu.

```
Switch(config)#interface fastethernet 0/1
switch(config-if)#switchport mode access //nastaví port do příslušného režimu
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum POČET_ADRES
Switch(config-if)#switchport port-security mac-address MAC_ADRESA_ZAŘÍZENÍ //manuální vložení adresy
Switch(config-if)#switchport port-security mac-address sticky //dynamické učení MAC adresy
Switch(config-if)#switchport port-security violation {shutdown | restrict | protect}
```

Ukázka konfigurace Port Security na přepínači Cisco

## 2. DHCP Snooping



DHCP Spoofing je druh síťového útoku, kdy útočník v lokální síti falšuje zprávy DHCP protokolu (např. spuštěním vlastního DHCP serveru s pozměněnými síťovými parametry) s cílem podvrhnout oběti např. jinou výchozí bránu. Tím může útočník docílit přesměrování provozu od oběti na svůj počítač. Následně je pak schopen odposlouchávat veškerý odchozí provoz od oběti.

---



Jiným typem útoku na DHCP server je vyčerpání adresních rozsahů DHCP serveru (DHCP Starvation). V tomto případě útočník generuje velké množství zfalšovaných žádostí o přidělení adresy, čímž dojde k jejich vyčerpání.

---

DHCP Snooping je označení postupů, kterými se lze bránit proti DHCP Spoofingu. Konfiguruje se na přepínačích, které jsou přímo připojeny ke koncovým stanicím (tzv. přístupové přepínače – Access Switches). Celý proces obrany proti DHCP spoofingu spočívá v odposlouchávání DHCP dotazů na portech přepínače, a blokování odesílání podvržených odpovědí dotazujícím se stanicím. Tím je vliv útočnickova podvrženého DHCP serveru eliminován. Odesílání odpovědí z DHCP

serveru je povoleno pouze na důvěryhodných (Trusted) portech přepínačů. To, který port je „důvěryhodný“ nastavuje ručně administrátor a obvykle to je pouze jeden port, ke kterému je připojen pravý DHCP server. Cisco přepínače umožňují nastavit DHCP Snooping pro libovolný počet VLAN, nastavit důvěryhodné porty, na nichž jsou připojeny DHCP servery, a omezit počet dotazů **PPS** (*Packet Per Second*) na DHCP serveru a zabránit tak jeho přetížení. Ukázka konfigurace DHCP Snoopingu je na následujícím výpisu.

```
Switch(config)#ip dhcp snooping
switch(config)#no ip dhcp snooping information option
Switch(config)#ip dhcp snooping vlan JEDNA_VLAN_NEBO_ROZSAH
Switch(config)#interface fastethernet ČÍSLO
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#ip dhcp snooping limit rate PPS //vypne option 82 - používá se pro DHCP Relay
```

Ukázka konfigurace DHCP Snoopingu na přepínači Cisco

Zapnutím funkce DHCP Snooping Binding Database (viz následující výpis), je možné se navíc chránit i před dalšími typy útoku v lokálních sítích. Po zapnutí této funkce si totiž přepínač vytváří tabulku obsahující vazby mezi MAC adresou stanice, IP adresou, dobou zapůjčení IP adresy, portem ze kterého komunikuje, virtuální sítí (VLAN) ve které se nachází a způsobem jakým byla položka do tabulky přidána (ručně nebo automaticky). Tyto informace pak využívá funkce **DAI** (*Dynamic ARP Inspection*), která chrání před útoky typu ARP Cache Poisoning.

```
Switch(config)#ip dhcp snooping database flash:/dhcpbind.txt
```

Zapnutí funkce DHCP Snooping Binding Database na přepínači Cisco

### 3. Dynamic ARP Inspection

$E=m \cdot c^2$

ARP Cache Poisoning je velmi jednoduše realizovatelný a těžko odhalitelný útok spočívající ve falšování odpovědí zpráv protokolu **ARP** (*Address Resolution Protocol*). Protokol ARP zajišťuje zjišťování vazeb IP adresa-MAC adresa v lokální síti. Útočník pomocí zfalšovaných odpovědí dokáže způsobit přesměrování komunikace napadeného PC na útočnicka. Následně pak může odposlouchávat kompletní komunikaci oběti s ostatními stanicemi v síti.



Tento útok lze detekovat (a zabránit mu) přímo na přepínači, který podporuje funkci DAI.



Útok lze jednoduše zrealizovat na PC např. nástrojem Cain&Abel ([www.oxid.it](http://www.oxid.it)) nebo Ettercap (<http://ettercap.sourceforge.net/>)

Funkce DAI je způsob obrany proti ARP Cache Poisoningu. Využívá se tabulky vytvořené pomocí DHCP Snoopingu. Pokud na přepínač přijde ARP paket z důvěryhodného (trusted) portu, je poslán dále. Pokud ovšem na přepínač přijde



ARP paket z nedůvěryhodného (untrusted) portu, je dále analyzován. Pokud se jedná o zprávu ARP Request, síťový procesor v paketu zjistí, zda-li MAC a IP adresa počítače žádajícího o překlad patří k sobě. Pokud ano, je paket přeposlán dál do sítě. V opačném případě je zahozen. V případě, že se jedná o odpověď na dotaz (ARP Reply), tak se navíc kontroluje, zda k sobě patří MAC a IP adresa počítače odpovídajícího na zprávu ARP Request. Kombinace IP a MAC adres jsou brány z databáze vytvořené funkcí DHCP Snooping. Příkaz pro zapnutí DAI je na následujícím výpisu.

```
Switch(config)#ip arp inspection vlan Vlan_ID //zapnutí funkce DAI
Switch#show ip arp inspection vlan Vlan_ID //zobrazení sledovaných VLAN
```

#### Zapnutí funkce DAI na přepínači Cisco

Na dalším výpisu je příkaz pro vypnutí kontroly DAI na důvěryhodných rozhraních.

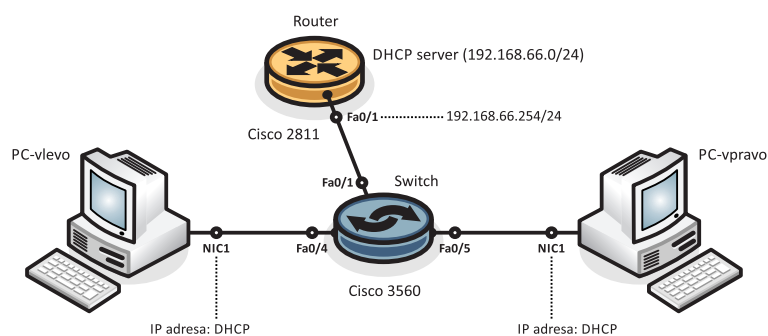
```
Switch(config)#interface fastethernet 0/1
Switch(config-if)#ip arp inspection trust //označení rozhraní jako důvěryhodného
```

#### Vypnutí kontroly DAI na důvěryhodném rozhraní přepínače Cisco

IP Source Guard má podobnou funkci jako DAI, ale místo zfalšovaných MAC adres se detekují zfalšované zdrojové IP adresy. Umožňuje blokování nepovolených IP adres na portech. Nastavuje se na konkrétní port. Tato funkce také využívá DHCP Snooping Binding Database. Příkaz pro zapnutí funkce IP Source Guard je na následujícím výpisu.

```
Switch(config)#interface JMÉNO_ROZHRAŇÍ
Switch(config-if)#ip verify source port-security //filtruje podle zdrojové IP a MAC adresy
```

#### Zapnutí funkce IP Source Guard na přepínači Cisco



Příklad topologie zapojení úlohy pro simulaci útoků v lokální síti

## 8 Budování VPN pomocí IPSec – příklady a řešení

Vzdálený přístup je dnes zcela neoddiskutovatelnou součástí správy síťových zařízení libovolně velké lokální sítě, a to především s ohledem na nutnost pohotového zásahu správce sítě v případě nenadálé situace a ve spojitosti se snížením celkových nákladů na takovou akci. Stačí tedy, aby byl správce sítě připojen k Internetu, a může tak vzdáleně monitorovat a případně rekonfigurovat jednotlivé síťové prvky.

V minulosti se pro vzdálený přístup ke správě síťových prvků používal protokol Telnet. Ten ovšem nijak nechránil vlastní komunikaci, takže bylo relativně snadné provoz odposlouchávat a zachytit přihlašovací informace. Rozšířením přístupu k Internetu tedy vznikla potřeba na takový protokol, který by veškerou komunikaci zabezpečil před potenciálními útočníky. Vznikl tak protokol **SSH** (*Secure Shell*), který standardně komunikuje transportním protokolem TCP na portu 22, poskytuje zabezpečenou autentizaci obou stran, zajišťuje jejich integritu, transparentní šifrování přenášených dat a volitelně i bezztrátovou kompresi (více informací lze nalézt v doporučení RFC 4252 [<https://www.ietf.org/rfc/rfc4252.txt>]).

Potřeby velkých společností vzájemně bezpečně propojit oddělené pobočky daly vzniknout virtuálním privátním sítím zajišťujícím propojení dvou a více síťových zařízení v prostředí nedůvěryhodné veřejné sítě Internet. Dalším důvodem byla i cena za propojení. V případě využití vyhrazených okruhů by totiž byly náklady nesrovnatelně vyšší. VPN lze obecně dělit podle vrstvy, na které pracují z pohledu referenčního modelu OSI. Nejpoužívanější VPN technologie přehledně uvádí následující tabulka.

## Nejpoužívanější technologie v sítích VPN

Typ VPN	Vrstva RM-OSI	Popis
Frame Relay	spojová	Vyžaduje homogenní prostředí Frame Relay. Spolehlivější, bezpečnější, ale i dražší v porovnání s IP VPN.
ATM	spojová	Vyžaduje homogenní prostředí ATM. Podobně jako FR poskytuje virtuální kanály se smluvenými parametry.
L2TP/PPTP	spojová	L2TP jako náhrada PPTP, které odvozuje klíče z hesla uživatele (potenciální slabina). PPTP využívá pro šifrování <b>MPPE</b> ( <i>Microsoft Point-to-Point Encryption</i> ) a L2TP IPsec. Definovány doporučeními RFC 2637 <a href="https://www.ietf.org/rfc/rfc2637.txt">[https://www.ietf.org/rfc/rfc2637.txt]</a> a RFC 2661 <a href="https://www.ietf.org/rfc/rfc2661.txt">[https://www.ietf.org/rfc/rfc2661.txt]</a> .
BGP/MPLS	spojová/síťová	Slouží k bezpečné výměně informací mezi hraničními směrovači <b>BGP</b> ( <i>Border Gateway Protocol</i> ) v páteřních sítích pomocí MPLS tunelů. Definován doporučením RFC 4364 <a href="https://www.ietf.org/rfc/rfc4364.txt">[https://www.ietf.org/rfc/rfc4364.txt]</a> a dalšími.
IPSec	síťová	Bezpečnostní rozšíření klasického protokolu IP. Šifrováním každého paketu vzniká transparentní zabezpečený přenos (tzv. tunel). Definován několika RFC doporučeními.
SSL/TLS	transportní a vyšší	<b>SSL</b> ( <i>Secure Sockets Layer</i> ) je technologie nezávislá (transparentní) na použité technologii síťové vrstvy. Ze SSL je následně odvozen protokol <b>TLS</b> ( <i>Transport Layer Security</i> ) definovaný v doporučení RFC 5246 <a href="https://www.ietf.org/rfc/rfc5246.txt">[https://www.ietf.org/rfc/rfc5246.txt]</a> .

Nejobvyklejším způsobem propojení poboček je dnes spojení pomocí protokolu IPSec VPN, kdy je sestaven šifrovaný jednosměrný logický (virtuální) kanál, tzv. SA, mezi směrovači/firewally umístěnými na perimetru lokální sítě.



Pro duplexní (obousměrnou) komunikaci je tedy třeba sestavit dvě nezávislé jednosměrné SA.



Protokol IPSec je povinnou součástí IPv6 a dodatečně byl implementován i do IPv4.

Umožňuje pracovat ve dvou režimech (tunelovacím – plně zapouzdřený původní IP paket do nového IP paketu, a transportním – záhlaví protokolu IPsec je vloženo mezi původní IP záhlaví a záhlaví protokolu vyšší vrstvy) a využívá pro zabezpečení dvou protokolů AH a ESP. Oba protokoly podporují buďto nulové šifrování (NULL), nebo algoritmy **DES** (*Data Encryption Standard*), **3DES** (*Triple DES*), **AES** (*Advanced Encryption Standard*) a Blowfish. Protokol IPsec je

definován v mnoha doporučeních **RFC (Request For Comments)**, ale nejzákladnější je doporučení RFC 4301 [<https://www.ietf.org/rfc/rfc4301.txt>]. Pro zajištění integrity jsou použity HMAC algoritmy **MD5 (Message-Digest 5)** a **SHA-1**.

## 8.1 Příklad konfigurace IPsec VPN na zařízeních fy.Cisco

V první fázi je třeba nastavit politiky IKE protokolu ISAKMP. Politika IKE slouží protokolu IPsec k sestavení SA. Pro jejich sestavení je však potřeba vyjednat sdílený klíč PSK mezi oběma stranami, ze kterého budou odvozeny vlastní šifrovací klíče. Pro výměnu klíčů je obvykle využít mechanismus DH. Protokol ISAKMP používá transportní protokol UDP na portu 500. Příklad konfigurace politik (typ autentizace, šifrovací a hashovací algoritmus, DH grupy a doby životnosti SA v sekundách) je patrný z následujícího obrázku.

```
Router(config)#crypto isakmp policy 1
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#encryption {des|3des|aes 128|aes 192|aes 256}
Router(config-isakmp)#hash {md5|sha}
Router(config-isakmp)#group {1|2|5}
Router(config-isakmp)#lifetime 86400
```

Konfigurace IKE politik protokolu ISAKMP na směrovači Cisco

Dále je třeba nastavit sdílený klíč PSK, kterým se strany vzájemně autentizují. V rámci příkazu je rovněž definována IP adresa druhé strany. Příklad je opět uveden na následujícím obrázku.

```
Router(config)#crypto isakmp key TADYjeTENTajnyKLIC address 192.168.0.2
```

Konfigurace sdíleného klíče PSK na směrovači Cisco

V druhé fázi se konfiguruje vlastní nastavení protokolu IPsec. Definuje se množina použitých algoritmů pro šifrování a zajištění integrity dat, tzv. **TS** (*Transform Set*). Pro příklad použijeme protokol ESP v kombinaci s HMAC algoritmem SHA-1. Směrovač začne příslušný provoz šifrovat až tehdy, pokud má nastavený tzv. zajímavý provoz (*Interesting Traffic*) pomocí klasického firewallovacího pravidla **ACL** (*Access List*). Takto definované parametry spojí objekt, tzv. kryptomapu (*Crypto Map*), která je spolu s dalšími dodatečnými parametry jako výchozí adresa druhé strany (obecně lze definovat více adres) a nepovinnými parametry jako DH grupa, doba životnosti IPsec SA (v sekundách) následně aplikována na příslušné rozhraní **WAN** (*Wide Area Network*). Vše je patrné z příkladu na následujícím obrázku.

```

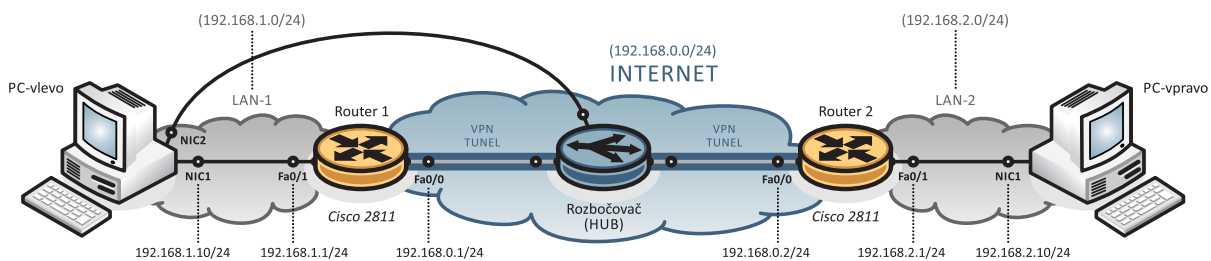
Router(config)#crypto ipsec transform-set ESP-AES esp-aes 256 esp-sha-hmac
Router(config)#ip access-list extended ZAJIMAVY-PROVOZ
Router(config-ext-nacl)#permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
Router(config)#crypto map IPSEC-MAPA 1 ipsec-isakmp
Router(config-crypto-map)#match address ZAJIMAVY-PROVOZ
Router(config-crypto-map)#set peer 192.168.0.2 default
Router(config-crypto-map)#set transform-set ESP-AES
Router(config-crypto-map)#set pfs group2
Router(config-crypto-map)#set security-association lifetime seconds 86400
Router(config)#interface fastethernet 0/0
Router(config-if)#crypto map IPSEC-MAPA

```

### Konfigurace protokolu IPsec VPN na směrovači Cisco



Analogicky je nutné obě IPsec fáze nastavit i na druhé komunikující straně (směrovači) !!!



Příklad topologie zapojení úlohy na IPsec VPN

## 9 Budování VPN pomocí SSL/TLS – příklady a řešení

Pomocí VPN nelze jen propojovat jednotlivé pobočky, ale také lze kontrolovaně zpřístupňovat klientům zdroje umístěné v nepřístupné části podnikové sítě pomocí protokolu **HTTPS** (*HyperText Transfer Protocol for Secure*) – protokol **HTTP** (*HyperText Transfer Protocol*) s podporou SSL/TLS. Klient se připojí pomocí běžného webového prohlížeče podporujícího SSL/TLS na vstupní webovou stránku, kde zadá své přihlašovací údaje. V případě, že jsou správné, je mu zpřístupněna stránka se sdílenými síťovými zdroji. Veškeré spojení je přitom zabezpečeno pomocí SSL/TLS.

Přístup SSL VPN řeší také některé nevýhody klasické IPSec VPN. IPSec VPN má problémy při průchodu přes NAT. To sice lze obejít mechanismem NAT-T, který spočívá v zabalení paketů IPsec resp. ESP paketů do datagramů UDP, nicméně to zvyšuje celkovou režii protokolu. Další nevýhodou je v případě vzdáleného přístupu k VPN nutnost speciálního programového vybavení na straně účastníka. Implementace IPsec klientů různých výrobců také nemusí být vzájemně kompatibilní, tunel nemusí jít sestavit kvůli bezpečnostním pravidlům v cizích sítích (např. filtrováním odchozího provozu, použitím proxy serverů), ...

Řadě těchto problémů se lze vyhnout použitím VPN využívajících protokol SSL/TLS. Tento VPN přístup je označován jako SSL VPN nebo také Clientless VPN, protože uživatel nepotřebuje speciální programové vybavení pro přístup k VPN, resp. využije běžný webový prohlížeč s podporou protokolu HTTPS.

Termínem SSL VPN je často označována řada vzájemně nekompatibilních technologií. Nicméně, všechny jsou postaveny na stejné základní myšlence a tou je využití asymetrické kryptografie a knihoven SSL/TLS pro zabezpečenou komunikaci. Technologie protokolů rodiny SSL/TLS je dnes hojně využívána při šifrovaném přístupu k webovému serveru schématem HTTPS.

Cílem SSL VPN je vytvoření transparentního šifrovaného tunelu založeného na protokolu SSL/TLS. Vzhledem k přítomnosti SSL v běžných webových prohlížečích není nutné pro dosažení většiny nabízené funkčnosti instalovat na klientské počítače žádný speciální klientský software. K rozšíření možností SSL VPN řešení jsou dále používány malé aplikace v podobě Java appletů nebo ActiveX komponent. Právě bohatost nadstandardní výbavy významně ovlivňuje užitnou hodnotu implementací SSL VPN od různých výrobců.

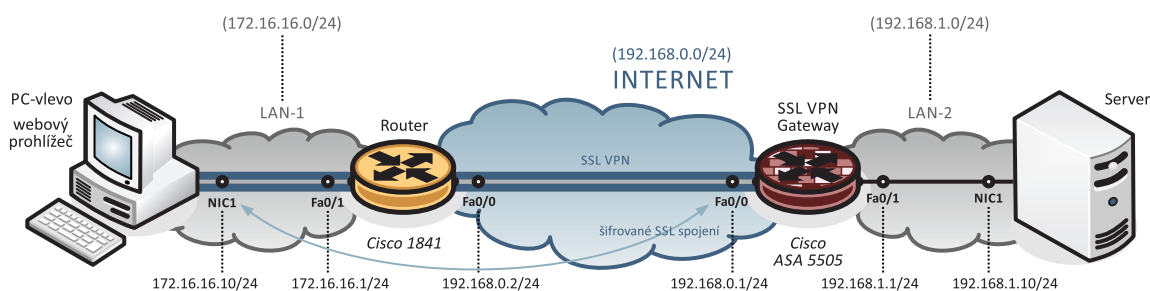
Základní funkcionalita SSL VPN spočívá v zabezpečeném přístupu k vnitřním informačním zdrojům organizace. Je vytvořen šifrovaný SSL tunel mezi SSL VPN bránou a webovým prohlížečem na klientském počítači. V této podobě tedy může SSL VPN velmi dobře posloužit jako implementačně jednoduchý způsob, jak v rámci internetu zabezpečeně zpřístupnit webové portály informačních systémů organizace. Další běžnou vlastností SSL VPN řešení je možnost, s pomocí bránou nabízeného webového rozhraní, pracovat se soubory sdílenými v rámci vnitřní sítě pomocí **CIFS** (*Common Internet File System*), tedy sdílení souborů novějších systémů Windows nebo unixového **NFS** (*Network File System*).

## 9.1 Typy přístupů SSL VPN

### 1. Clientless VPN

V tomto režimu vzdálený uživatel přistupuje do interní sítě použitím internetového prohlížeče (FireFox, Chrome, Internet Explorer, Edge, Safari,...) na klientském počítači (viz obrázek níže). Vzdálený uživatel má dostupné aplikace:

- internetové prohlížení (používající HTTPS) – portálová stránka poskytuje seznam URL webových serverů, které může vzdálený uživatel prohlížet
- sdílení souborů (používající souborový systém CIFS) – portálová stránka poskytuje seznam souborových serverů, kde může vzdálený uživatel:
  - prohlížet a stahovat sdílené soubory,
  - přejmenovávat a mazat soubory,
  - nahrávat a stahovat soubory a
  - vytvářet a přejmenovávat nové soubory a adresáře.



Příklad topologie zapojení úlohy na IPSec VPN

### 2. ThinClient

Zásadní podmínkou je, že počítač vzdáleného uživatele musí tento způsob komunikace podporovat. Vzdálený uživatel si z portálové stránky stáhne Java applet. Tento applet funguje na klientovi jako TCP proxy server pro služby, které jsou nakonfigurovány na portálové stránce. Tento typ umožňuje vzdálený přístup jak ke standardním aplikacím založeným na TCP jako jsou **POP3** (*Post Office Protocol 3*), **SMTP** (*Simple Mail Transfer Protocol*), **IMAP** (*Internet Message Access Protocol*) nebo Telnet, jakož i přístup k podnikovým informačním systémům typu **SAP** (*System Application Products*). Klientské aplikace musejí být nakonfigurovány tak, aby komunikovaly přes TCP spojení na známý server a port. Jako adresa serveru obvykle slouží loopback (127.0.0.1), kde je komunikace zachytávána TCP proxy serverem a dále směrována do SSL tunelu.



### 3. Tunnel

V tomto režimu má vzdálený uživatel největší možnosti. Uživatel si po přihlášení na VPN serveru stáhne (ručně nebo automaticky) plnohodnotného SSL VPN klienta. V případě technologie Cisco jde o „Cisco AnyConnect VPN klient“. Tento program vytvoří virtuální síťové rozhraní, které poskytuje přístup k síťové vrstvě různým aplikacím. Tento typ SSL VPN poskytuje možnosti srovnatelné s VPN na technologii IPsec (v režimu vzdáleného přístupu - Remote Access). Po ukončení spojení se Cisco AnyConnect VPN klient odstraní z klientské stanice nebo může zůstat na stanici nainstalován.



---

Klasické SSL VPN nelze použít k vytváření Site-to-Site VPN, používají se většinou jako Remote-Access VPN. Výjimkou z tohoto pravidla je projekt OpenVPN, který umožňuje vytvářet Site-to-Site VPN zabezpečené pomocí SSL/TLS.

---

## 10 Elektronický podpis

Důvodů pro zavádění elektronického podpisu je hned několik. Jednak vznikla nutnost zavedení ekvivalentu ke klasickému podpisu, za druhé dnes vzniká velký počet dokumentů v elektronické podobě, resp. některá data dokonce existují pouze v digitální podobě a především svou podstatou výrazně omezuje jejich snadné padělání.

Obecně je u elektronického podpisu nutné zajistit identifikaci podepisující osoby/subjektu, neporušenost doručeného dokumentu (datovou integritu), nepiratelnost a právní akceptovatelnost.

U elektronicky podepsaného dokumentu můžeme dále vyžadovat utajení vlastního obsahu zprávy (tj. šifrování) a zjištění, zda dokument existoval v konkrétním čase (tj. časové razítko).

Co je to vlastně elektronický podpis? Definice elektronického podpisu vychází z nařízení Evropského parlamentu a Rady EU č. 910/2014 o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním evropském trhu (ve zkratce **eIDAS** (*electronic IDentification, Authentication and trust Services*))

$E=m \cdot c^2$

Nařízení eIDAS definuje v čl. 3 odst. 10 elektronický podpis jako údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené. Elektronický podpis tedy slouží jako metoda k jednoznačnému ověření totožnosti podepsané osoby ve vztahu k datové zprávě.



Této velmi obecné definici vyhoví i podpis textem obyčejného e-mailu.

Elektronický podpis má hned několik možných variant:

- elektronický podpis,
- zaručený elektronický podpis,
- uznávaný elektronický podpis a
- kvalifikovaný elektronický podpis.

*i*

Pojem uznávaný elektronický podpis je české specifikum (do 09/2018). Jedná se o zaručený elektronický podpis založený na kvalifikovaném certifikátu. Je tedy použitelný pro komunikaci s orgánem veřejné moci **OVM** (avšak pouze v ČR!) a není zde vyžadována podmínka na zabezpečené HW úložiště. U kvalifikovaného elektronického podpisu musí být klíče naopak uloženy na „bezpečném“ prostředku.

Ve spojitosti s elektronickým podpisem je vhodné zmínit ještě pojem digitální podpis. Digitální podpis využívá prostředků asymetrické kryptografie. Jedná se tedy o konkrétní technické řešení elektronického podpisu.



---

Digitální podepisování chápeme dnes jako bezpečnostně nejlepší způsob realizace elektronického podepisování.

---



---

Pojem elektronický podpis je v kontextu digitálního podpisu pojmem obecnějším, je totiž technologicky neutrální. Zahrnuje v sobě kromě digitálního podpisu i všechny ostatní metody zajišťující požadované vlastnosti (např. biometrické metody). Z tohoto důvodu je použitelným i pro legislativní dokumenty.

---

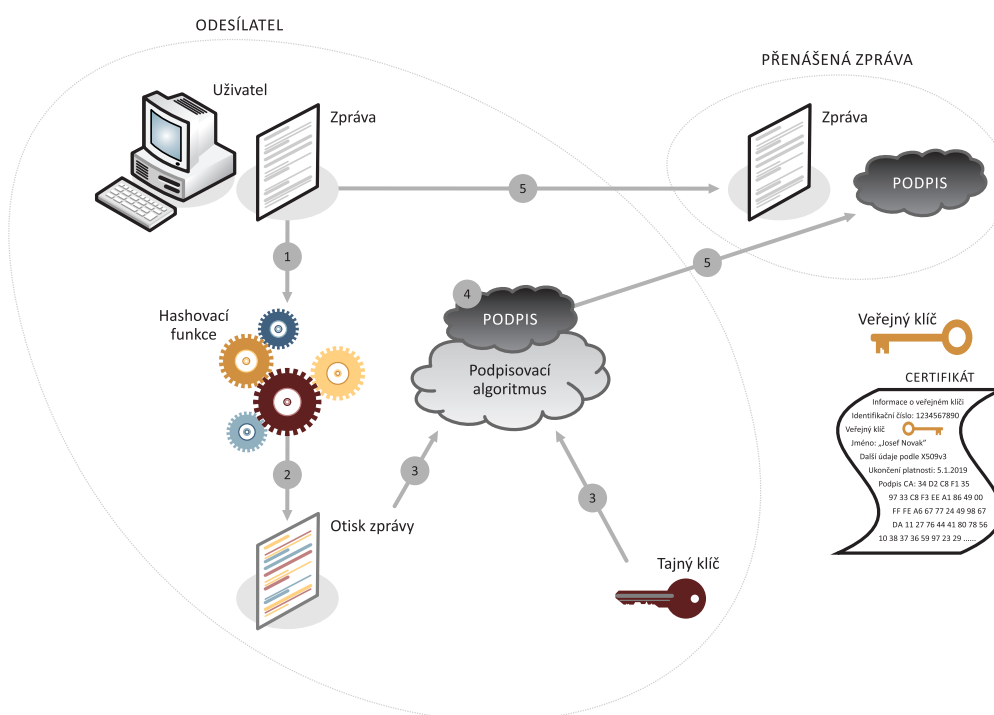


- 
1. Digitální podpis je pojem kryptologický, resp. matematický.
  2. Elektronický podpis je pojem zejména právní a normotvorný.
  3. Samotná definice elektronického podpisu stanovuje požadavky, ale neřeší, jak jich dosáhnout.
  4. Nástroje pro digitální podpis se naopak plně soustředí na plnění stanovených požadavků.
-

## 10.1 Zaručený elektronický podpis

Z kryptografického hlediska je elektronický podpis chápán jako soustava dílčích kryptografických funkcí zabezpečujících identifikaci, autentizaci, integritu a nepopíratelnost. Matematicky je elektronický podpis svým vyjádřením pouze jedno velké číslo.

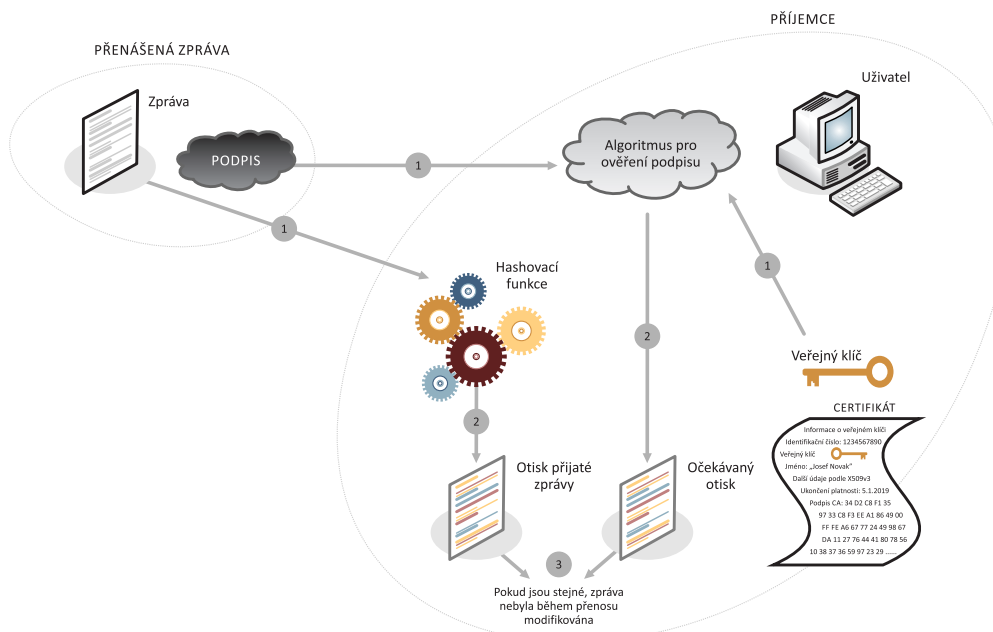
Na následujícím obrázku je znázorněn proces vytvoření zaručeného elektronického podpisu. Čísla v obrázku indikují jednotlivé kroky procesu tvorby zaručeného elektronického podpisu.



Proces vytvoření zaručeného elektronického podpisu

Elektronicky lze podepsat libovolná digitální data jako je např. text (PDF, TXT, DOCX, RTF, XLSX,...), obrázek (BMP, JPG, GIF, PNG,...), audio (WAV, MP3, FLAC,...), video (AVI, MPG,...), spustitelné soubory (EXE, COM,...) a další. Ve své podstatě tedy cokoliv.

Na následujícím obrázku je znázorněn proces ověření zaručeného elektronického podpisu. Čísla v obrázku indikují jednotlivé kroky procesu ověření zaručeného elektronického podpisu.



Proces ověření zaručeného elektronického podpisu



Zaručený elektronický podpis zajišťuje integritu přenášených zpráv a dokumentů, identifikaci komunikujících stran, autentizaci komunikujících stran (tj. ověření jejich identifikace) a nepopiratelnost, resp. neodmítnutelnost.



Zaručený elektronický podpis naopak nezajišťuje právní akceptovatelnost podepsaných dokumentů.



Nařízení eIDAS definuje zaručený elektronický podpis v čl. 3 odst. 11, resp. splňuje-li podmínky uvedené v čl. 26:

1. Je jednoznačně spojen s podepisující osobou.
2. Umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě.
3. Byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou.
4. Je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat.

## 10.2 Kvalifikovaný elektronický podpis



---

Nařízení eIDAS definuje kvalifikovaný elektronický podpis v čl. 3 odst. 12 jako zaručený elektronický podpis, který je vytvořen kvalifikovaným prostředkem pro vytváření elektronických podpisů, a který je založen na kvalifikovaném certifikátu pro elektronické podpisy.

---



---

Má stejnou platnost jako vlastnoruční podpis.

---



---

Kvalifikovaný certifikát je definován nařízením eIDAS v čl. 3 odst. 15 jako certifikát pro elektronický podpis, který je vydán kvalifikovaným poskytovatelem služeb vytvářejících důvěryhodné certifikáty a splňuje požadavky stanovené v příloze I daného nařízení.

---



---

Technicky je kvalifikovaný certifikát stejný jako libovolný „běžný“ certifikát.

---

## 10.3 Elektronická pečeť

Technologicky jde o totéž jako v případě zaručeného elektronického podpisu. Rozdíl je v oblasti jejího využití, která je zaměřena na právní rovinu.



---

Elektronický podpis používá výhradně fyzická osoba, elektronická pečeť může být využita výlučně právnickou osobou nebo organizační složkou státu.

---



---

Dříve byl pro elektronickou pečeť používán termín elektronická značka. Ve své podstatě se jedná o ekvivalent úředního razítka, které garantuje integritu a původ dokumentu.

---

Kvalifikovaná pečeť je založena na kvalifikovaném elektronickém podpisu, resp. je jeho ekvivalentem s ohledem na oblast jejího využití (výlučně pro právnické osoby). Dále vyžaduje specifický HW modul **HSM** (*Hardware Security Module*) pro uložení soukromého (tajného) klíče.

---



Druhy certifikátů z hlediska elektronického podpisu:

1. osobní, tj. určené pouze pro fyzické osoby
    - a) komerční – zákon nespécifikuje jejich obsah, využívány např. pro přihlašování do datových schránek
    - b) kvalifikovaný – určený pro podepisování zpráv a dokumentů
  2. systémový, tj. určený pro právnické osoby, organizační složky státu nebo orgány veřejné moci
    - a) komerční – využití např. pro přihlášení do spisové služby
    - b) kvalifikovaný – určený pro vytváření elektronických pečetí
-

## 10.4 Časové razítko

$E=m \cdot c^2$

Časové razítko prokazuje existenci dokumentu v dané podobě v pevně specifikovaném čase, tzn. neřeší se, kdy dokument vznikl a kdo dokument vlastnil.

Datová struktura časového razítka je obdobná jako struktura certifikátu. Technicky je časové razítko realizováno jako další elektronický podpis odvozený od autority časových razítek **TSA** (*Time Stamp Authority*).

*i*

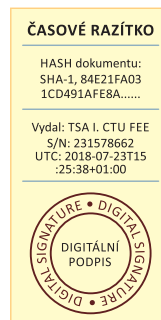
Existuje i tzv. kvalifikované časové razítko jakožto ekvivalent kvalifikované elektronické pečeti, resp. kvalifikovaného elektronického podpisu. Kvalifikované časové razítko vytváří kvalifikovaný poskytovatel služby časových razítek.

Elektronicky podepsaná struktura časového razítka mimo jiné obsahuje:

- jméno vydavatele,
- jedinečné sériové číslo razítka,
- kontrolní součet (tzv. HASH) odvozený z dokumentu a
- čas



Autorita časových razítek TSA prokazuje synchronizaci svého časového zdroje s celosvětovým časovým standardem **UTC** (*Universal Time Coordinated*).



Ukázka časového razítka