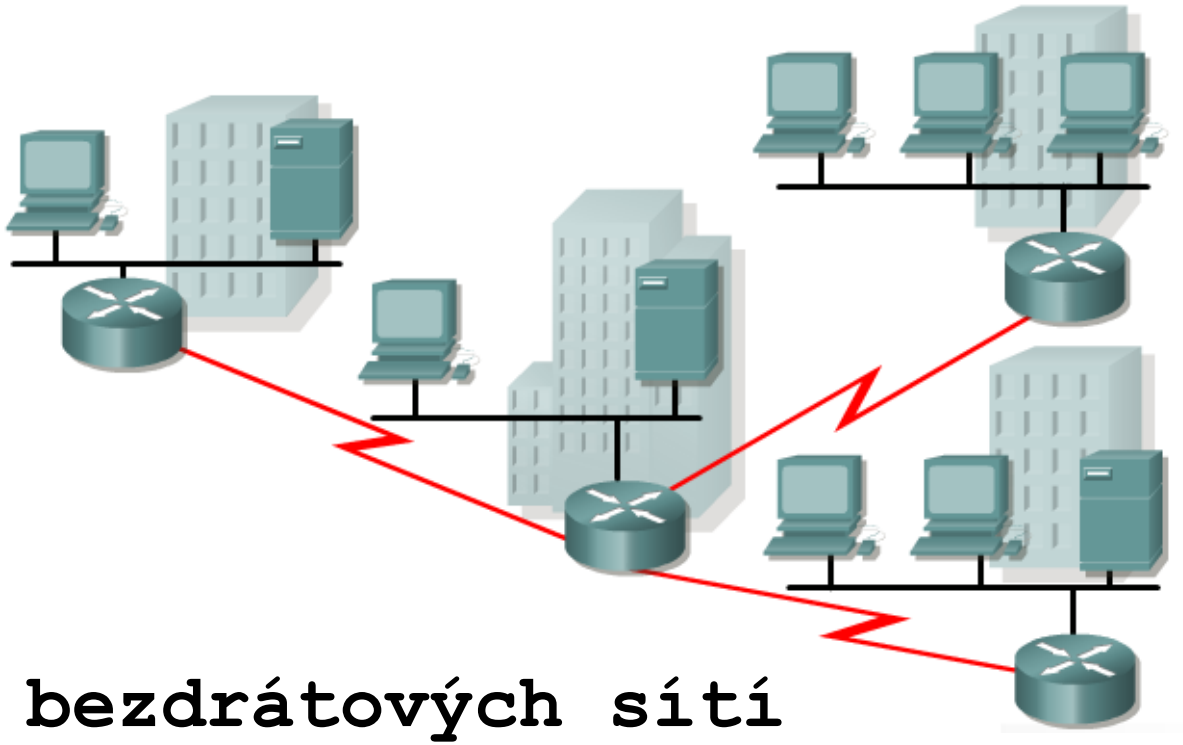


Zabezpečení bezdrátových sítí
IEEE 802.11, 802.16, 802.15

Ing. Tomáš Vaněk tomas.vanek@fel.cvut.cz

Osnova

- Bezpečnostní protokoly používané v sítích 802.11
  - WEP
  - WPA-TKIP
  - IEEE 802.11i (WPA2)
  - IEEE 802.1x
- Zabezpečení v IEEE 802.16 (WiMAX)
- Zabezpečení v IEEE 802.15 (Bluetooth)

Proč je otázka zabezpečení u bezdrátových sítí tak důležitá ?

U bezdrátových sítí nelze dostatečně omezit přístup k fyzickému médiu.

Základní atributy bezpečnosti, které je nutné zajistit:

- Autentizace a Autorizace
- Integrita
- Utajení

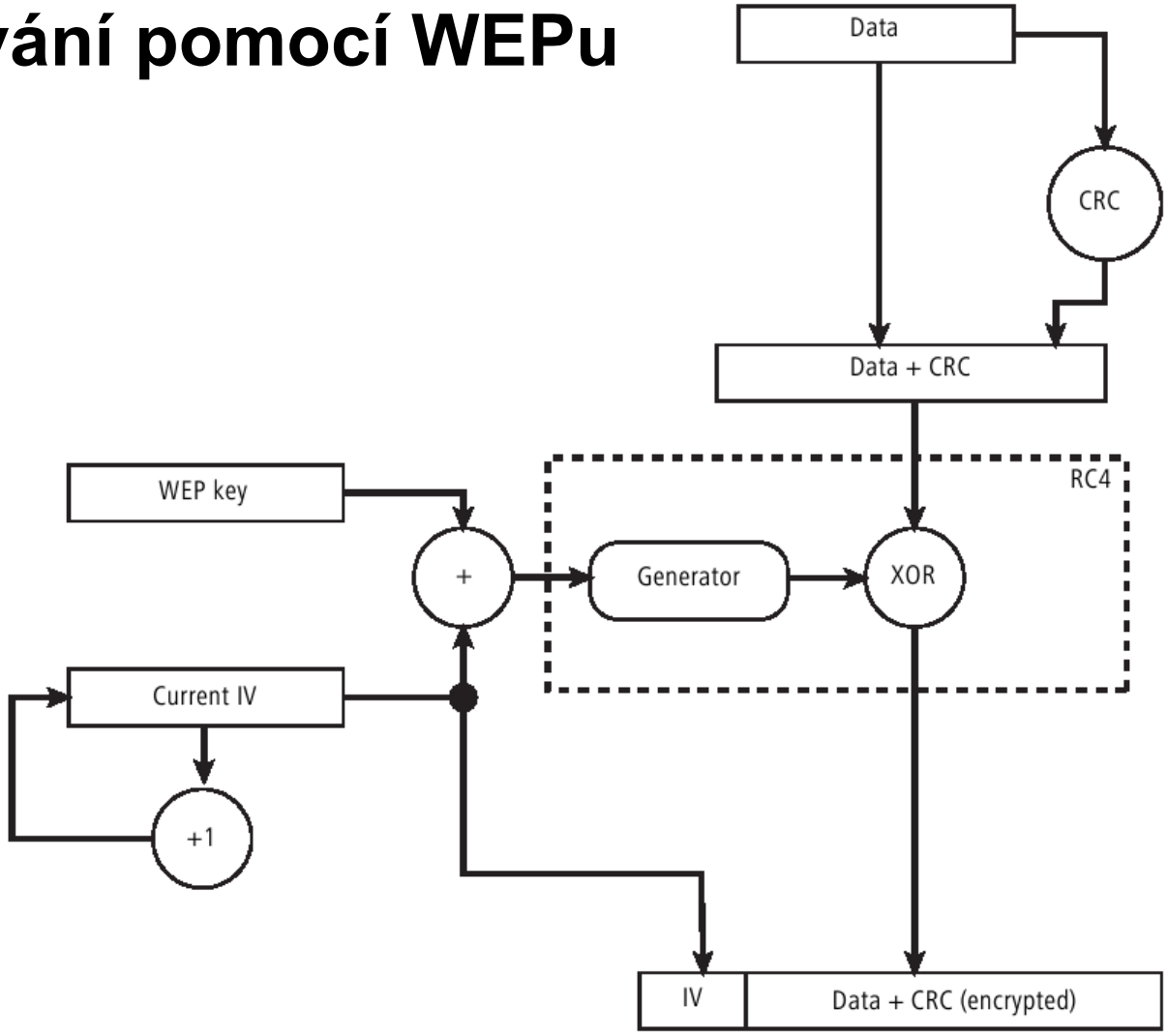
WEP

- WEP je protokol zajišťující nepovinné zabezpečení sítí 802.11
- doslova „soukromí jako v drátových sítích“
- hlavní cíl: utajit přenášená data
- obsah datových rámců je zašifrován algoritmem RC4
- datové rámce jsou chráněny před změnou pomocí CRC-32 (Cyclic Redundancy Check)
- volitelná autentizace na základě znalosti sdíleného klíče
- široce podporovaný, ale snadno prolomitelný
- délka klíče 64 bitů (dle standardu, v praxi se používají i 128 a 256 bitů)

RC4

- symetrická proudová šifra
- základem je tabulka o velikosti 255 bajtů
- v každém kroku RC4 dojde k
  - prohození prvků v současné tabulce
  - výběru bajtu klíče z tabulky
- počáteční nastavení (permutace) je dána klíčem
- RC4 podporuje klíče délky 8-2048 bitů
- v každý krok RC4 produkuje 8 bitů proudu klíče

Šifrování pomocí WEPu



Implementace RC4 do WEPu

- hlavním problémem není použitý algoritmus, ale jeho implementace do systému
- délka klíče 64, 128 nebo 256 bitů
- 24 bitů klíče tvoří vždy Iniciační vektor – IV
- Reálná délka klíče je tedy 40, 104 nebo 232 bitů
- klíč je stejný pro každé zařízení v síti
- klíče jsou statické
- IV se přenáší v rámci v otevřeném tvaru
- IV se v každém rámci mění
- WEP klíč lze spočítat po odposlechnutí dostatečného počtu rámců (statisíce až milióny)

Hlavní nedostatky WEPu

- délka klíče (64 bitů)
- neexistence správy klíčů (nutnost manuální výměny, modifikace,…)
- malá velikost IV (pouze 24 bitů ->2^{24} kombinací)
- nedostatečná ochrana integrity (pouze pomocí CRC-32)
- špatná implementace RC4 do WEPu (existence slabých klíčů - 9000 z 2^{24} možných)
- slabá autentizace pomocí sdíleného klíče

- Pracovní skupina 802.11 vyvíjela doporučení 802.11i, které problematiku bezpečnosti řeší komplexně
- Do doby než byla 802.11i přijata byly uvolněny hotové části 802.11i jako tzv. WPA (WiFi Protected Access)

FMS útok

- 2001 – popsány slabiny v práci s klíči u algoritmu RC4
- 2004 – popsán útok na protokol WEP schopný získat klíč
- Fluhrer, Mantin, Shamir
- pasivní odposlech provozu
- první byty OT většiny paketů jsou snadno předpověditelné (hlavičky protokolů LLC, IP)
- IV se přenáší v otevřeném tvaru -> lze dešifrovat první tři byty z každého paketu
- zbývající byty klíče jsou konstantní pro všechny pakety

FMS útok

- v dalších krocích se útočník snaží zrekonstruovat RC4 KSA (Key Schedule Algorithm)
- pro určitou malou skupinu IV existuje asi 5% pravěpodobnost, že budou vyhovovat tzv. podmínce F_{fms} a umožní odhalit další byte klíče.
- při zachycení cca 4-6x10^6 paketů je 50% pravděpodobnost odhalení klíče

- PODROBNOSTI viz. „útoky na WEP a WPA.pdf“

KoreK útok

- 2004
- hacker KoreK
- 16 dalších korelací mezi prvními *L* byty RC4 klíče, prvními dvěma byty generovaného proudu klíče a dalším bytem klíče K[*L*].
- útok je podobný FMS, ale efektivnější
- při zachycení cca $7x10^5$ paketů je 50% pravděpodobnost odhalení klíče
- konkrétní hodnoty závisejí na implementaci protokolu
- např. jestli jsou IV generovány nějakým PRNG algoritmem (a jakým), nebo se mění sekvenčně

PTW útok

- 2007
- Tews, Weinmann, Pyshkin
- výrazné urychlení
- při zachycení cca $4x10^4$ paketů je 50% pravděpodobnost odhalení klíče, pro $6x10^4$ paketů je 80% a pro $8,5x10^4$ paketů je 95%.
- v síti s větším provozem lze odchytat dostatečné množství paketů a následně zjistit klíč do 60 s

Chopchop útok

- aktivní útok
- útočník dokáže zjistit *m* posledních bytů OT ze zašifrovaného paketu odesláním průměrně 128*m* paketů (max. 256*m*) do sítě
- útočník nedokáže zjistit klíč
- útok není založen na slabinách implementace algoritmu RC4
- útočník ořízne paket o 1 byte, zrekonstruuje k takto odhadnutému paketu CRC a paket odešle
- pokud byl odhad nesprávný je i CRC špatné a paket je tiše zahozen
- pokud byl odhad správný je správné i CRC a paket je zpracován, ale protože mu poslední byte (nebo více) chybí AP ho zahodí a pošle chybovou zprávu

WPA – WiFi Protected Access

WPA

- zveřejněn v roce 2002
- dočasné řešení od Wi-Fi Alliance před schválením standardu 802.11i (červen 2004)
- stejný algoritmus jako u WEPu – RC4
- autentizace podle 802.1x založená na protokolu EAP (Extensible Auth. Protocol - RFC 2284)
- WEP nahrazen protokolem TKIP (Temporary Key Integrity Protocol)
- k CRC32 přidán další zabezpečující kód - MIC (Message Integrity Check)
- kompatibilní se stávajícími zařízeními - podporu WPA šlo přidat upgradem firmware

TKIP - Temporary Key Integrity Protocol

- nahrazuje protokol WEP
- stejný šifrovací algortimus (RC-4)
- na rozdíl od WEPu podporuje dynamické klíče

TKIP paket obsahuje

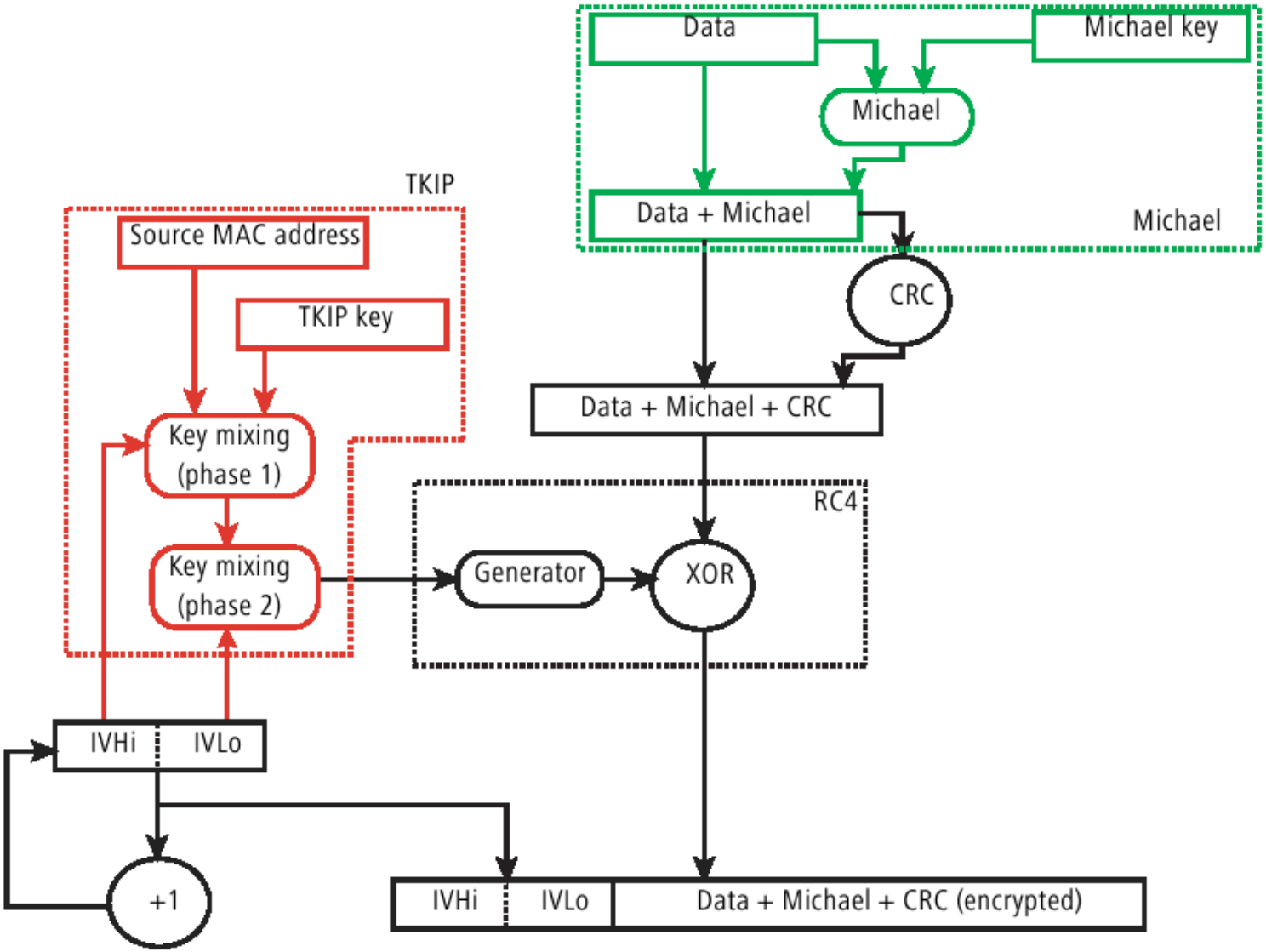
- klíč délky 128 bitů (PK – Packet Key)
- IV délky 48 bitů
- MAC adresu komunikujícího zařízení

- Klíč se mění každých 10000 paketů.
- Šifrovací algoritmus zůstává stále RC4 -> kompatibilita se starším HW, nutný pouze upgrade SW

MIC - Message Integrity Check

- rychlý algoritmus Michael
- 64bitový klíč
- MIC dohromady s CRC-32 řeší problém s možností záměny bitů v rámci
- 32bitové číslo spočtené z náhodného čísla, datového obsahu rámce, záhlaví a sequence number rámce.
- zabraňuje také vícenásobnému použití IV (replay útoky)
- rámce mimo pořadí jsou zahozeny

Jak to funguje

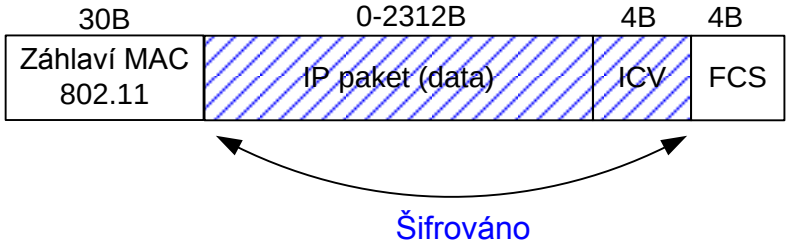


802.11i (WPA2)

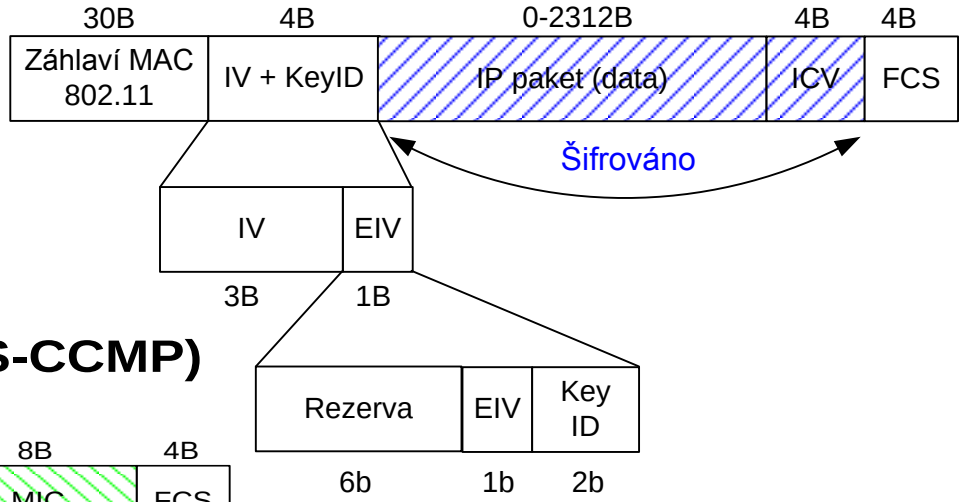
802.11i (WPA2)

- řeší komplexně problematiku zabezpečení v sítích IEEE 802.11
- zpětná kompatibilita s WPA (WPA je podmnožinou WPA2)
- WPA-PSK - alternativní možnost autentizace pro malé sítě
- nový šifrovací algoritmus – AES v režimu CCMP
- Broadcast Key Rotation (dříve pouze proprietární technologie Cisca)
- stávající zařízení nelze upgradovat softwarově

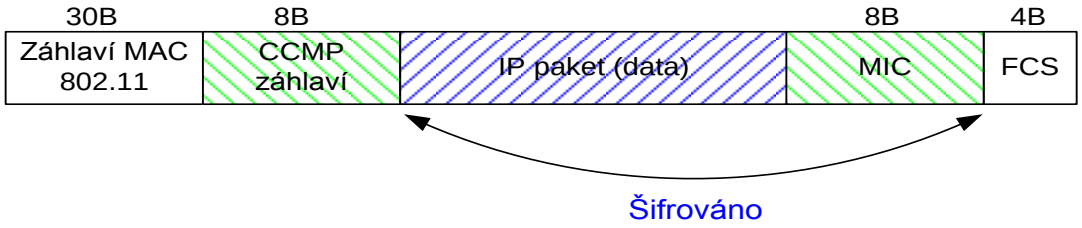
Nešifrováno



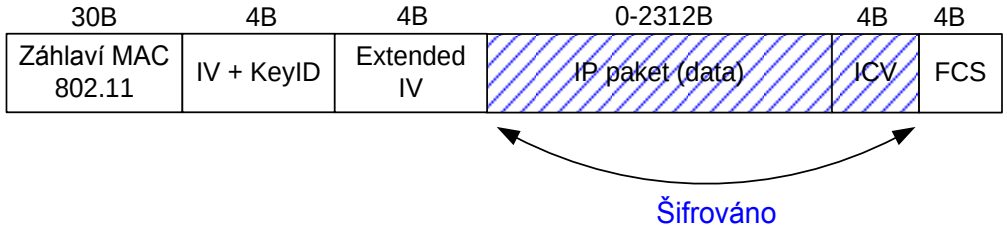
WEP



WPA-2/802.11i (protokol AES-CCMP)



WEP



Přehled možných autentizačních mechanismů v bezdrátové síti

1. Otevřená síť
2. Otevřená síť + autentizace pomocí MAC adresy
3. Otevřená síť + autentizace na VPN gatewayi
4. Otevřená síť + autentizace pomocí webového formuláře
5. Autentizace pomocí WEPu (sdílený klíč)
6. Autentizace pomocí WPA-PSK
7. Autentizace pomocí IEEE 802.1X

Autentizace

1. Otevřená autentizace (Open)

- AP autentizuje klienta na základě údajů přijatých ze stanice, ale tyto nijak neověřuje
- Každá stanice, která zná SSID je úspěšně autentizována

2. Otevřená síť + autentizace podle MAC adresy

- stejné jako varianta 1) + kontrola zdrojové MAC adresy
- problém s aktualizací databáze MAC adres na více AP
- lze jednoduše padělat

3. Otevřená síť + autentizace na VPN gatewayi

- samotná síť autentizaci neřeší
- klient se autentizuje na VPN gatewayi
- na straně klienta je potřeba příslušný SW (VPN klient)
- omezení na konkrétního výrobce
- obtížná rozšiřitelnost
- VPN-koncentrátotry jsou drahé

4. Otevřená síť + autentizace webovým formulářem

- po připojení do sítě je veškerý provoz přesměrován na přihlašovací stránku
- zde se uživatel autentizuje
- až po úspěšné autentizaci, je možné využívat síťové připojení
- počítač musí být vybavený WWW prohlížečem, který musí být po celou dobu spojení zapnutý
- příklad takovéto autentizace - eduroam-simple

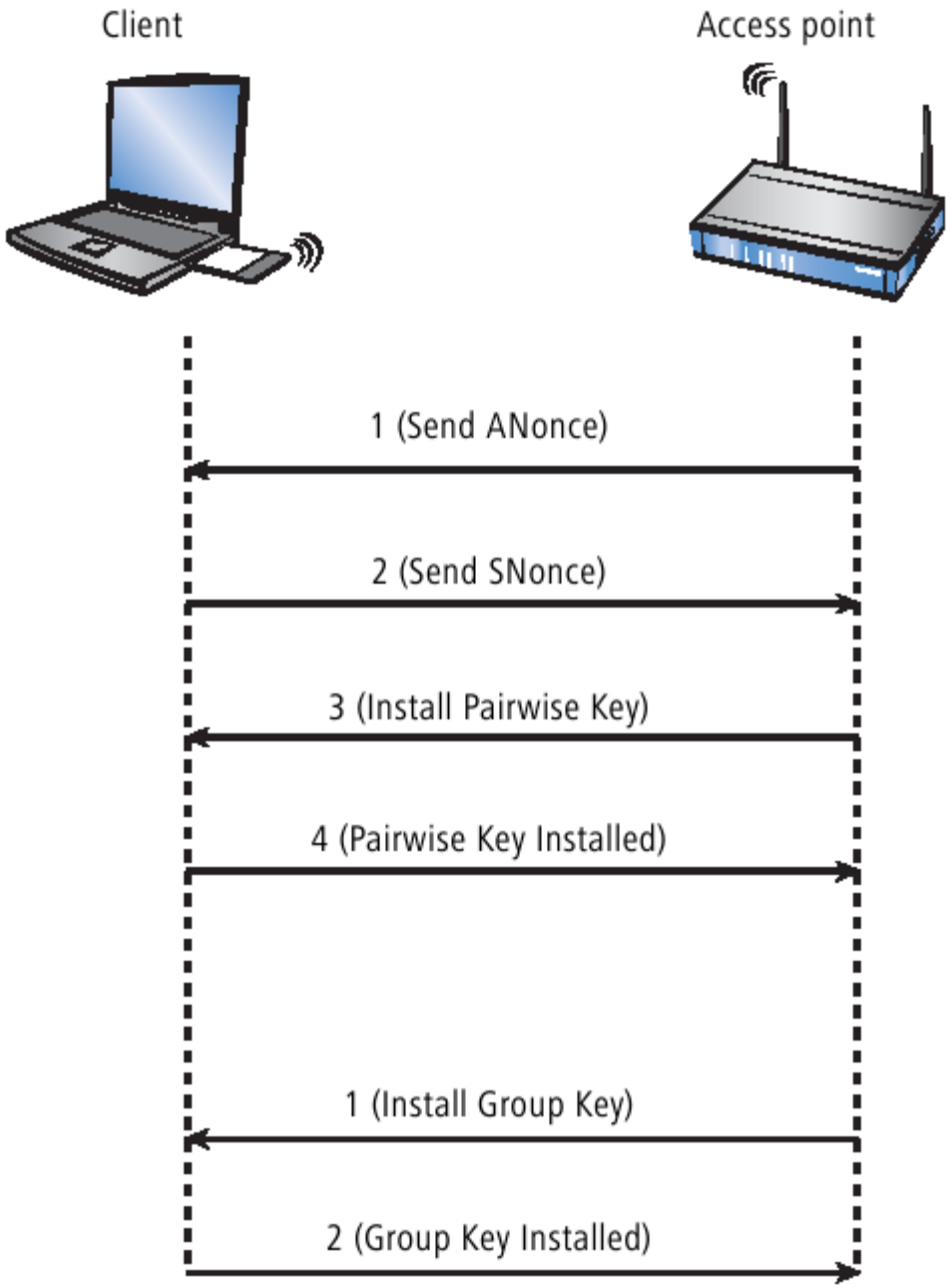
5. Autentizace sdíleným klíčem (Shared Key)

- klient vyzve přístupový bod (AP) k odeslání výzvy
- AP pošle klientovi náhodnou 128-bytovou výzvu
- klient zašifruje výzvu pomocí WEPu a sdíleného klíče
- klient odešle zašifrovanou výzvu odešle do AP
- pokud AP správně dešifruje svoji původní výzvu, povolí klientovi přístup

6. WPA-PSK (Pre-shared Key)

- alternativa ke správě klíčů pomocí 802.1X
- vhodné pro malé (domácí sítě)
- PSK je 256 bitové číslo nebo passphráze délky 8 - 63 znaků, která se pak na PSK převádí.
- Náchylnost na slovníkové útoky, nutno zvolit dostatečně dlouhou a složitou passphrázi
- PSK může být různý pro každé zařízení (v závislosti na MAC adrese)
- standardně výrobci používají jeden PSK pro celou síť

Předání klíčů AP->klient ve WPA-PSK



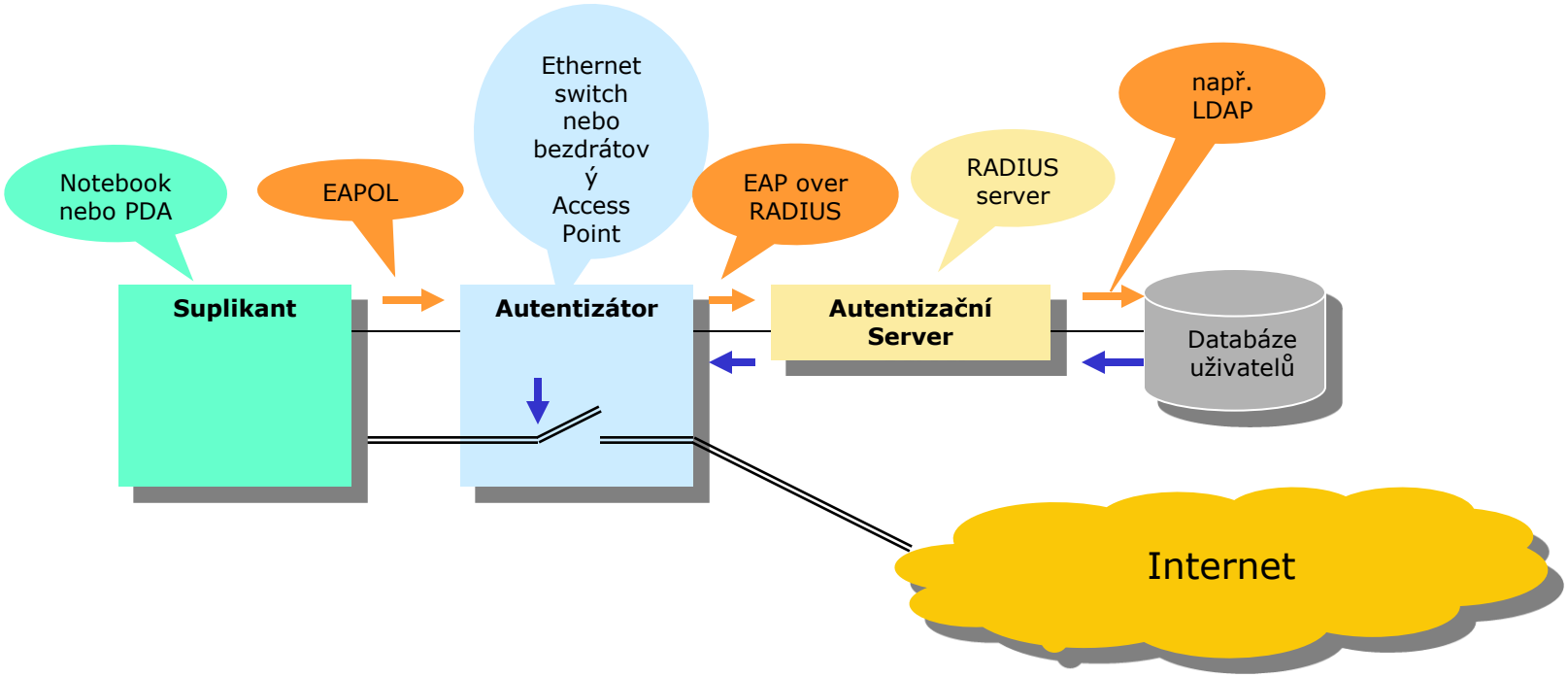
7. IEEE 802.1x

IEEE 802.1X je obecný bezpečnostní rámec pro všechny typy LAN, zahrnující autentizaci uživatelů, integritu zpráv, šifrování a distribuci klíčů.

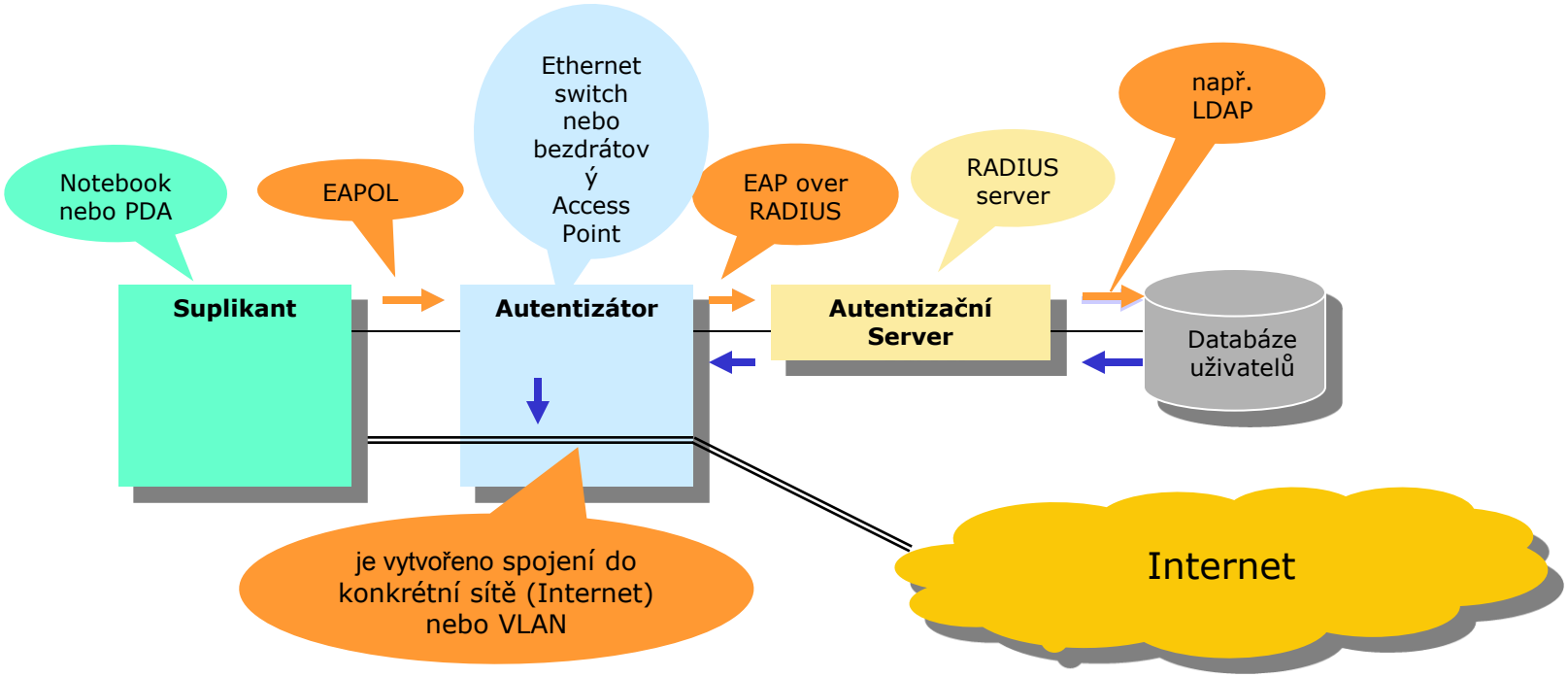
Architekturu IEEE 802.1x tvoří tři funkční entity:

- suplikant připojení k síti,
- autentizátor zajišťující řízení přístupu,
- autentizační server provádějící autorizační rozhodnutí.

Princip 802.1x



Princip 802.1x



Celý proces výměny klíčů

Suplikant
Auth/Asociováný
802.1X Neblokuje
PTK/GTK

Authentizátor
Auth/Asociováný
802.1X Neblokuje
PTK/GTK

Autentizační server (RADIUS)
Žádný klíč

Asociace 802.11

Autentizace pomocí
EAP/802.1X/RADIUS

MSK

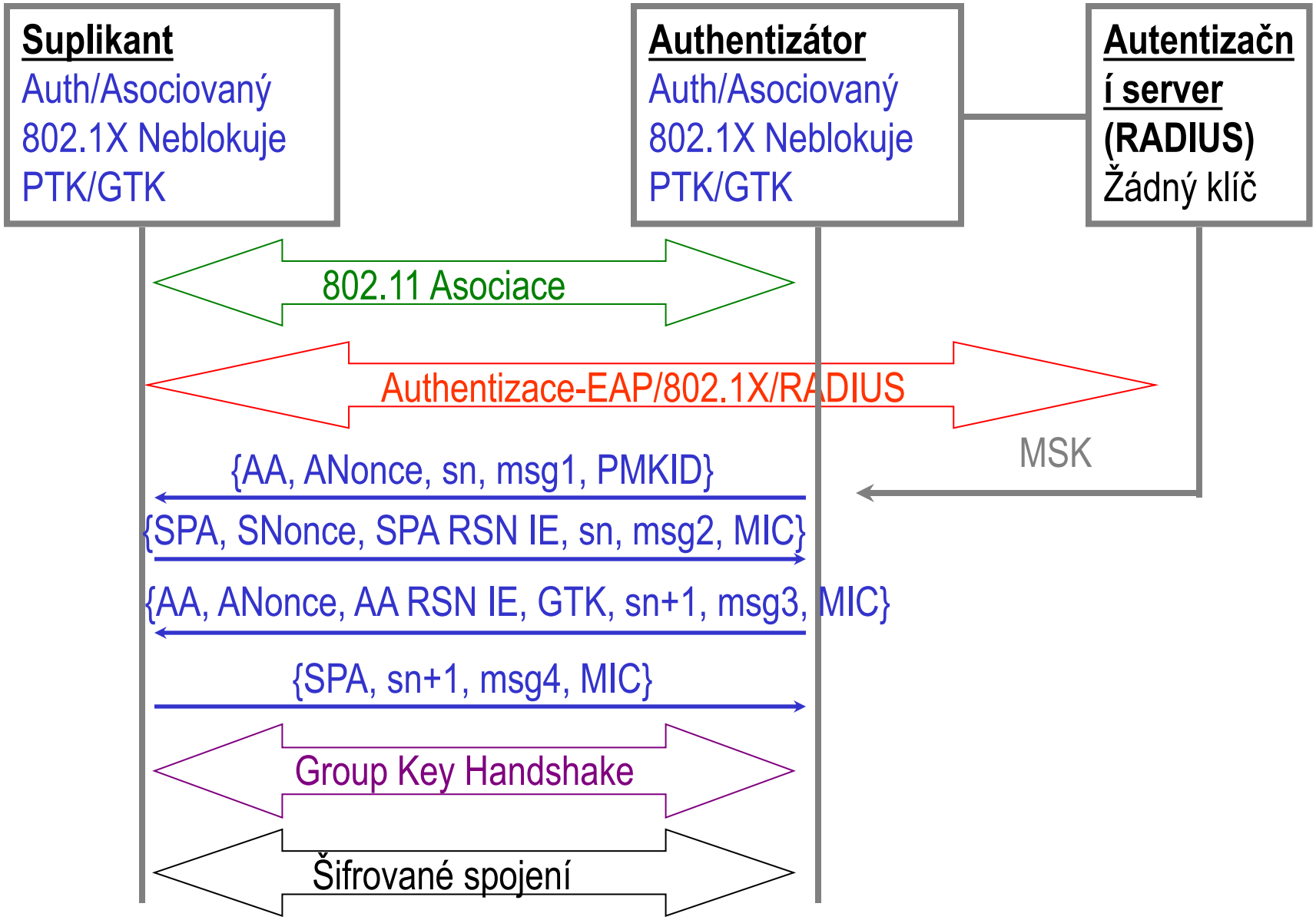
4-Way Handshake

Group Key Handshake

Šifrovaná komunikace

MSK … Master Session Key
PMK…Pair-wise Master Key
PTK…Pair-wise Transient Key
GTK…Group Transient Key

4-Way Handshake



4-way handshake

- 4-way handske slouží k odvození PTK (Pairwise Transient Key) a GTK (Group TK)
- PTK a GTK se odvozují z PMK (Pairwise Master Key), který se získá následovně:
  1) pokud je autentizace WPA-PSK pak PMK=PSK* pak má délku 512b
  2) pokud je autentizace 802.1x
     odvodí se z 802.1x MSK (Master Session Key) a PMK má délku 384b

PMK obsahuje:

KCK – Key Confirmation Key – 128b – klíč pro zajištění integrity během fáze 4-way handshake

KEK – Key Encryption Key – 128b – klíč pro šifrování dat během 4-way handshake

TK – Temporary Key – 128b – klíč pro šifrování protokolem TKIP nebo AES-CCMP

TMK1, TMK2 – Temporary Mic Key – 2x64b – klíč pro MIC – pouze u PSK

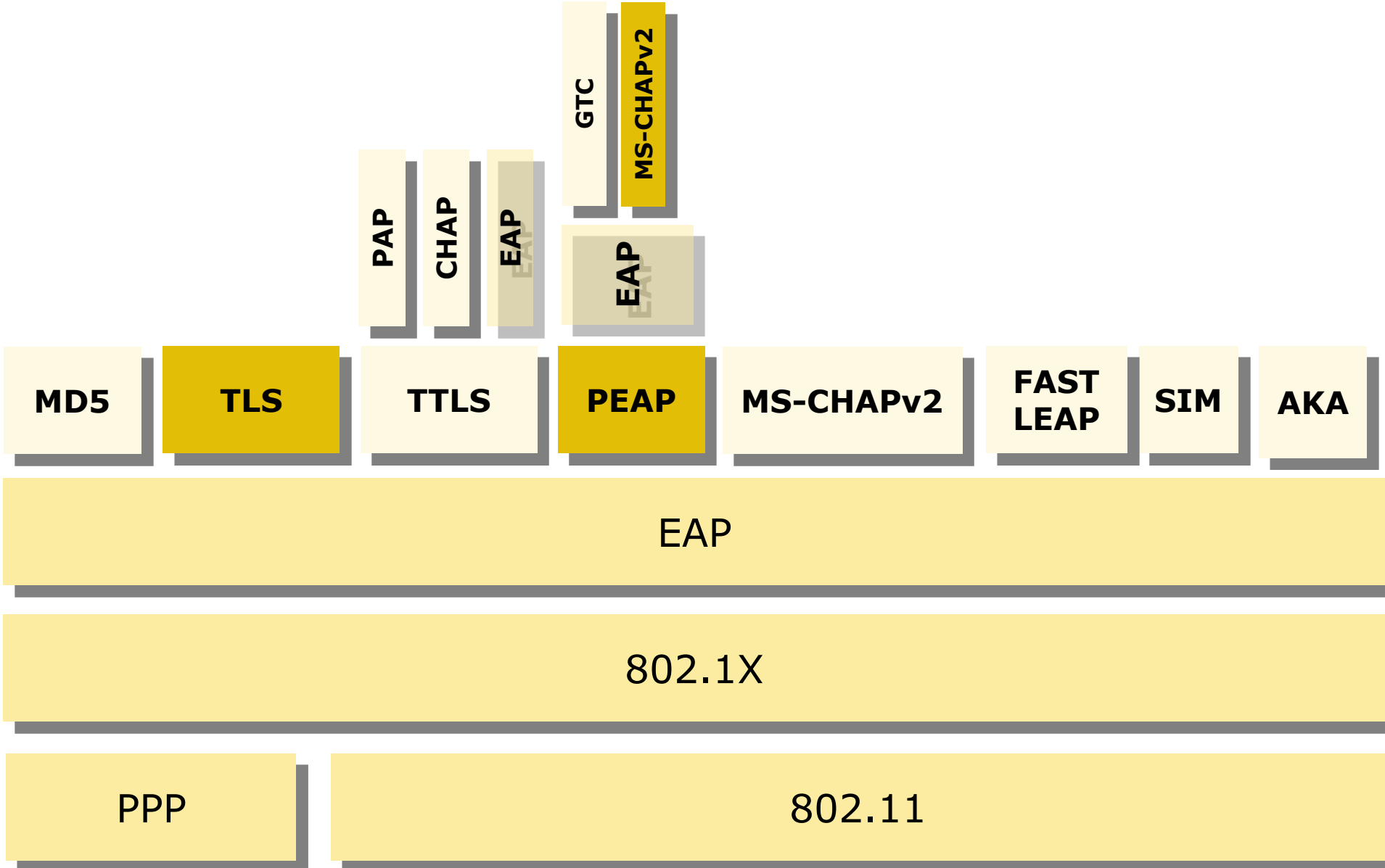
*PSK – Pre-Shared Key - generuje se z hesla (8-63 znaků)

4-way handshake

- po 4-way handshaku následuje GK Hansdhake
- po výměnu broadcast a multicast zpráv je nutné si vyměnit GTP (Group Transient Key)
- GTP = GEK + GIK
- GEK – Group Encryption Key – 128b - klíč pro TKIP nebo AES-CCMP
- GIK – Group Integrity Key – 128b - pouze pro algoritmus Michael (u TKIPu)

Obecný EAP (Extensible Authentication Protocol)

- AP vyšle po asociaci klienta EAP REQUEST-ID
- Klient odpoví EAP RESPONSE-ID, obsahující identifikační údaje uživatele
- AP 'přebalí' tuto zprávu do paketu RADIUS ACCESS_REQUEST a pošle RADIUS serveru
- RADIUS server odpoví RADIUS ACCESS_ACCEPT nebo DENY, což AP 'přebalí' pro klienta jako EAP SUCCESS / FAILURE
- Pokud je autentizace úspěšná, tak port, přes nějž tato komunikace probíhala, je otevřen pro datovou komunikaci klienta


GTC
MS-CHAPv2
PAP
CHAP
EAP
EAP
MD5
TLS
TTLS
PEAP
MS-CHAPv2
FAST
LEAP
SIM
AKA
EAP
802.1X
PPP
802.11

802.1x

802.1x využívá protokol EAP (Extensible Authentication Protocol) původně vyvinut pro PPP LCP (Point-to-Point Protocol - Link Control Protocol).
- zprávy EAP se zapouzdřují do rámců 802.1x

Varianty protokolu EAP:

EAP-MD5 (Message Digest 5)

- tato varianta EAP umožňuje pouze jednosměrnou autentizaci klienta.
- server odešle náhodné číslo (challenge)
- klient spočte hash: MD-5(challenge,heslo)
- pokud útočník může získat výzvu i odpověď lze použít slovníkový útok
- server se neautentizuje -> spoofing
- EAP-MD5 nelze vyžít k distribuci klíčů
- Závěr – EAP-MD5 lze použít v LAN ale ne v WLAN

LEAP (Lightweight EAP)

- vzájemná autentizace klienta a serveru
- proprietární protokol firmy Cisco
- označován také jako EAP-Cisco Wireless
- podobný EAP-MD5
- jsou k dispozici nástroje pro získání hesel

EAP-TLS (Transport Layer Security)

- nejbezpečnější, nejdražší na implementaci
- vzájemná autentizace pomocí certifikátů a protokolu TLS
- server používá TLS k dokázání vlastnictví digitálního certifikátu a to samé požaduje od klienta
- klient používá svůj certifikát k prokázání své identity a k výměně dat pro generování klíčů
- po úspěšné autentizaci je tunel ukončen, ale klíče odvozené během EAP-TLS se používají k šifrování pomocí AES, TKIP nebo WEP.

EAP-SIM (Subscriber Identity Module)

- vzájemná autentizace na základě SIM karty (nebo obecně nějaké smart-karty)
- požadavky na autentizaci podle 802.1X jsou přenášené protokolem EAP-SIM přes GW operátora do AuC příslušné GSM sítě.
- předpokládané použití při autentizaci smartphonů roamujících mezi WiFi a GSM sítěmi.

EAP-AKA (Authentication and Key Agreement)

- stejné jako EAP-SIM, ale pro sítě UMTS používající USIM (User Service Identity Module)
- používá silnější autentizační prostředky než EAP-SIM

EAP-FAST (Flexible Authentication via Secure Tunneling)

- vytvořilo Cisco jako náhradu LEAP
- vzájemná autentizace
- použití zabezpečeného tunelu (stejně jako EAP-TTLS nebo PEAP)
- EAP-FAST nevyžaduje, aby se server autentizoval pomocí certifikátu
- pro pomalé klienty typu WiFi telefony, kde by ověřování digitálních certifikátů trvalo dlouho
- v současnosti je použití omezeno pouze na WiFi sítě se zařízeními od firmy Cisco

EAP-TTLS (Tunneled TLS)

- AP se autentizuje pomocí má certifikátu
- klient nemá certifikát, autentizuje se pomocí protokolu PAP/CHAP(jméno/heslo), který je zapouzdřen v SSL tunelu
- proprietární protokol firem Funk Software a Certicom
- existují dvě verze:

  EAP-TTLSv0 …RFC5281

  EAP-TTLSv1 … nyní ve stádiu draftu IETF *http://tools.ietf.org/html/draft-funk-eap-ttls-v1-00*
- v praxi se neuplatnil
- nahradil ho EAP-PEAPv0/MSCHAP-v2

PEAP (Protected EAP)

- velmi podobný EAP-TTLS
- pouze server se autentizuje certifikátem
- TLS spojení pro bezpečnou autentizaci klienta
- otevřený standard vyvinutý firmami Microsoft, Cisco a RSA Security

Od 05/2005 je možné používat dvě varianty PEAP k autentizaci podle WPA/WPA2:

1) PEAPv1/EAP-GTC
2) PEAPv0/EAP-MSCHAPv2

PEAPv1/EAP-GTC (Generic Token Card)

- vyvinulo Cisco
- umožňuje používání jiných vnořených autentizačních protokolů než jen MSCHAPv2
- definuje obálku EAP pro přenos jednorázových hesel generovaných zařízeními jako je „RSA Secur ID“
- vhodné pro dvoufaktorovou autentizaci
- MS ho nikdy neimplementoval do Windows
- Cisco má své proprietární protokoly LEAP a EAP-FAST a také moc nepropaguje PEAPv1
- protože žádný OS nemá nativní podporu PEAPv1 takřka se nepoužívá se

PEAPv0/EAP-MSCHAPv2

- 2. nejrozšířenější po EAP-TLS, vyvinul ho Microsoft
- MS neuznává PEAPv1, proto označuje protokol PEAPv0 pouze jako PEAP (tzn. neuvádí v0 a v1)
- známe implementace : **AEGIS**
  - Windows
  - od firmy Meetinghouse

xsupplicant

- všechny POSIX (Linux, BSD, Unix like OS)
- projekt Open1x.org

Kromě těchto verzí existují i jiné varianty PEAP:

PEAP-EAP-TLS

- velmi podobný EAP-TLS
- autentizace klienta pomocí certifikátu, přes kanál šifrovaný pomocí TLS
- podporuje ho MS, ale ne Cisco a většina výrobců
- takřka se nepoužívá

PEAPv0-EAP-SIM / PEAPv1-EAP-SIM

- podporuje Cisco, ale ne MS
- vytvořen pro GSM sítě
- autentizace SIM karty v síti
- WiFi aliance se snaží rozšířit podporu EAP i mimo klasické bezdrátové sítě , zatím nepříliš úspěšně
- není nativně podporován v žádném OS

	EAP-MD5	LEAP	EAP-TLS	EAP-TTLS	PEAP
Autentizace Serveru	--	hash hesla	veřejný klíč (certifikát)	veřejný klíč (certifikát)	veřejný klíč (certifikát)
Autentizace klienta	hash hesla	hash hesla	veřejný klíč (certifikát nebo Smart karta)	CHAP, PAP, MS-CHAP(v2)	EAP-MS-CHAPv2 nebo veřejný. klíč
Dynamické Posílání klíčů	ne	ano	ano	ano	ano
Poznámka	Nejjedno-dušší a nejslabší varianta	LEAP = Lightweight EAP	TLS = Transport Layer Security	TTLS = Tunelled TLS	PEAP = Protected EAP

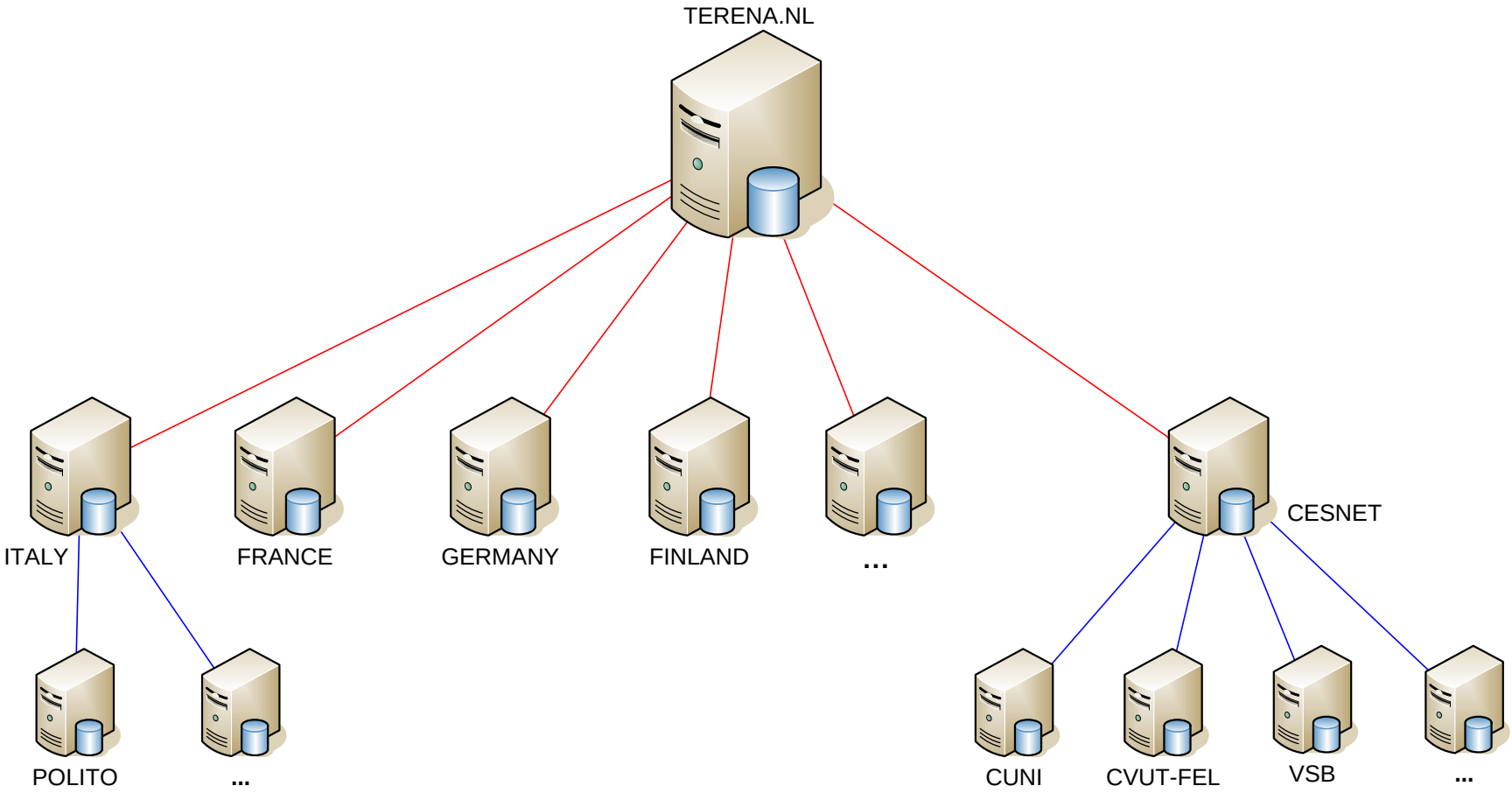
Varianty EAP schválené pro WPA/WPA2 :

- EAP-TLS
- EAP-TTLS/MSCHAPv2
- PEAPv0/EAP-MSCHAPv2
- PEAPv1/EAP-GTC
- EAP-SIM

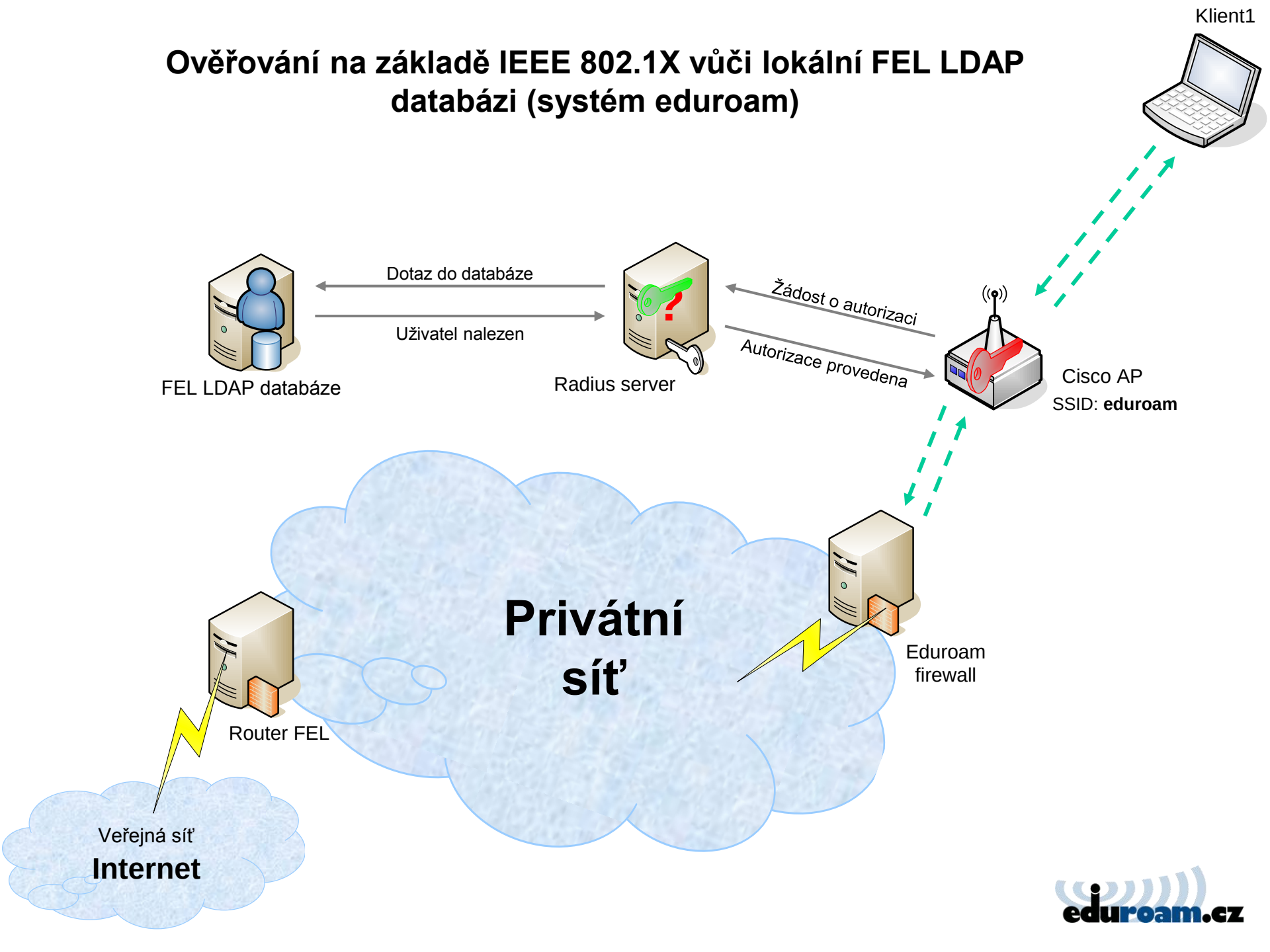
Příklad autentizace pomocí 802.1x v projektu eduroam

- eduroam - mezinárodní projekt zabývající se mobilitou a roamingem v počítačových sítích
- praktický příklad IP roamingu mezi organizacemi
- v ČR ho koordinuje CESNET
- Uživatel, který má účet pouze u jedné takové organizace (domovské síti) má oprávnění použít kteroukoliv síť organizace zapojené do projektu eduroam.
- ověřování se děje pomocí RADIUS serverů
- hiearchická struktura (podobně jako u DNS)
- směrování autentizačních požadavků na základě tzv. realmů
- uživatelské jméno má tvar username@realm
- realm – libovolný řetězec, v praxi shody s doménovým jménem instituce např. vanekt1@fel.cvut.cz

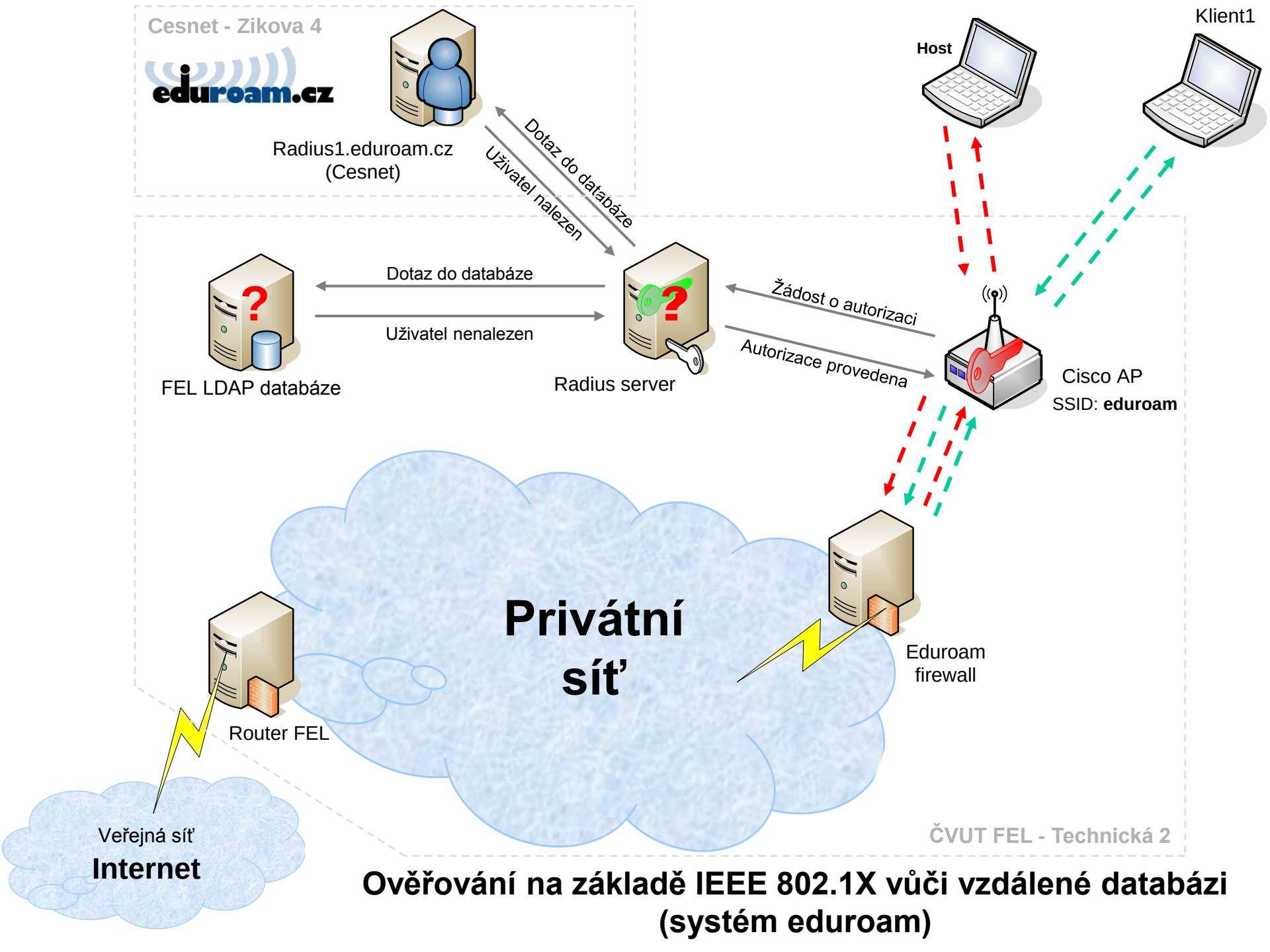
Struktura RADIUS serverů v rámci projektu eduroam



Ověřování na základě IEEE 802.1X vůči lokální FEL LDAP databázi (systém eduroam)

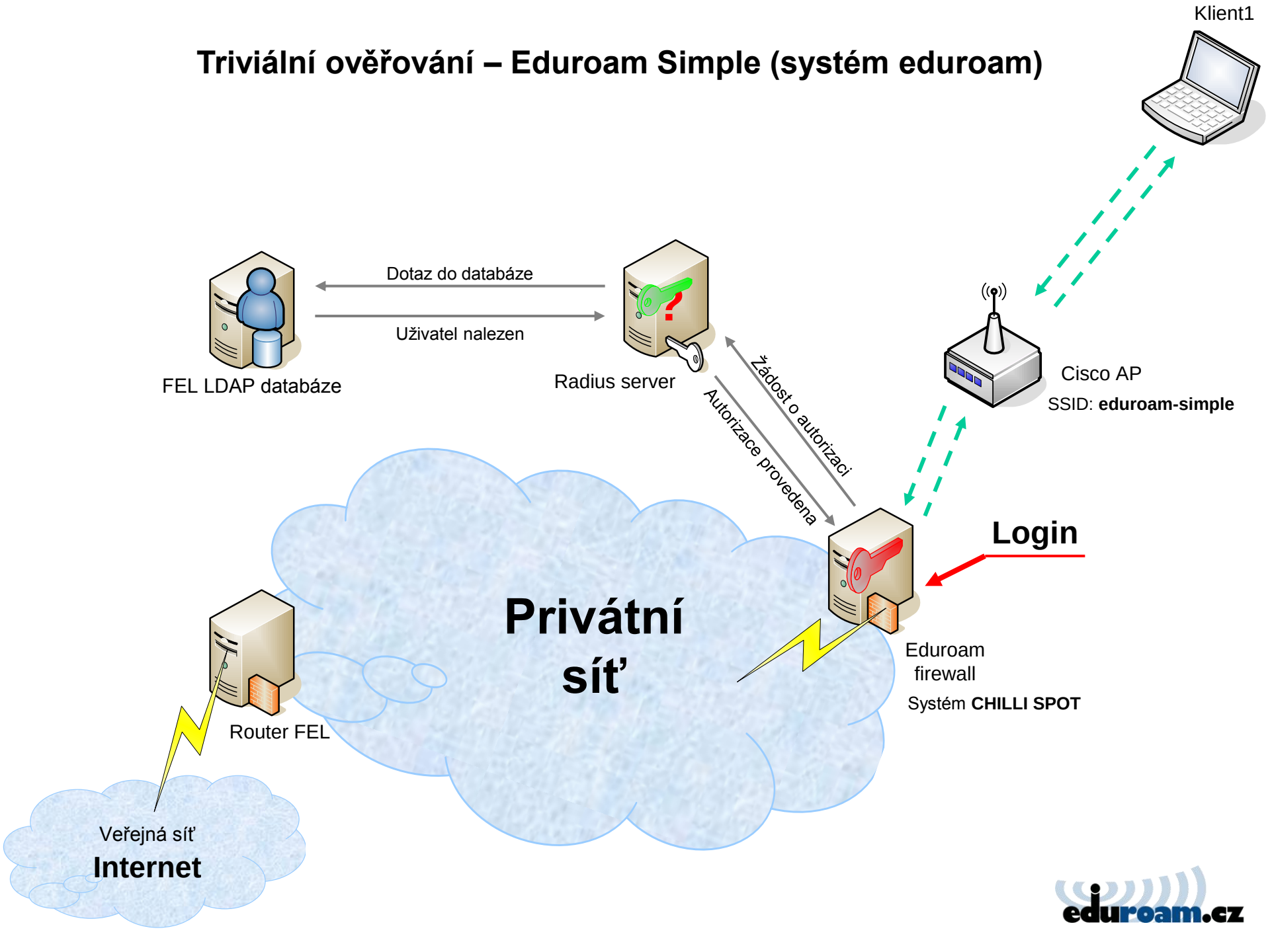


eduroam.cz



Ověřování na základě IEEE 802.1X vůči vzdálené databázi (systém eduroam)

Triviální ověřování – Eduroam Simple (systém eduroam)



DoS útoky sítě 802.11

- i při použití 802.11i je síť stále zranitelná těmito typy útoků!
- falšování nechráněných řídících rámců typu Deauthentication/Disassociation
- narušování řízení přístupu k médiu pomocí falšování rámců RTS/CTS
- možné řešení - autentizace řídících rámců
- DoS útoky na zprávy EAP - padělání zpráv EAPOL-Start, EAPOL-Success, EAPOL-Logoff, EAPOL-Failure
- současné poslání více než 255 požadavků na asociaci vedoucí k vyčerpání pole „EAP identifier“ (8 bitů)

Útoky na algoritmus Michael

DoS útok narušováním zpráv algoritmu

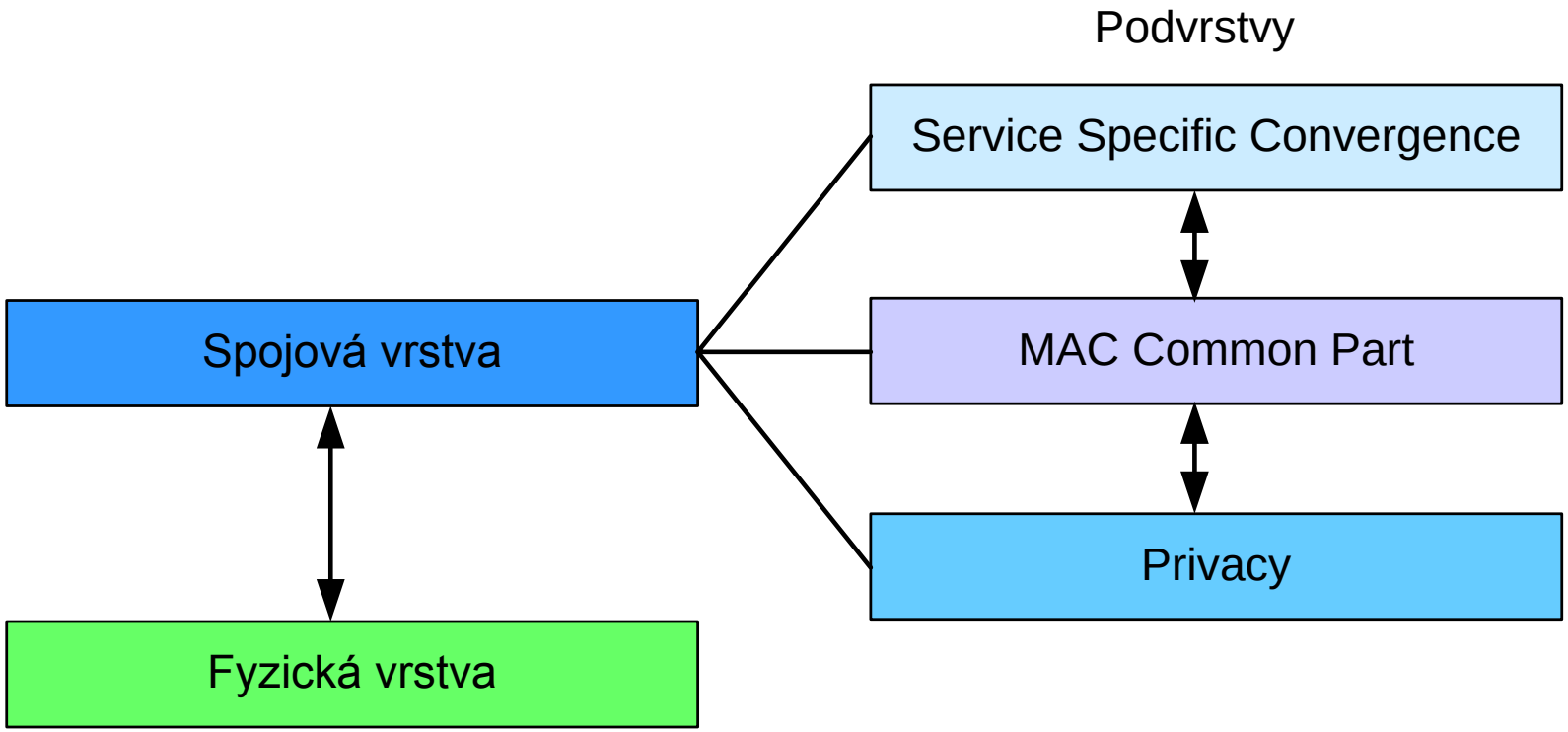
- zachycení paketu s platným TSC (TKIP Sequence Counter)
- modifikace paketu a vygenerování správných hodnot FCS, ICV
- odeslání modifikovaného paketu 2x za minutu
- MIC bude vždy neplatný, zatímco TSC vždy platný
- pokud síť detekuje dvě chyb algoritmu Michael za minutu přeruší na 60s komunikaci, poté následuje deautentizace a nové vygenerování šifrovacích klíčů
- omezení na 1 narušení za 6 měsíců (MIC má 20 bitů, existuje 2^{20} kombinací a lze vyzkoušet 2 kombinace za minutu)

Šifrovací algoritmy v bezdrátových sítích IEEE 802.16 (WiMAX)

Srovnání WiFi-WiMAX

802.11	802.16
Fixní šířka kanálu – 20MHz	Flexibilní šířka kanálu od 1,5 do 20 MHz
MAC vrstva je navržena pro desítky pracujících uživatelů	MAC vrstva je navržena pro tisíce pracujících uživatelů
	Šíři kanálu si může zvolit operátor
Neexistence QoS (řeší až 802.11e)	Od počátku podporuje QoS, DiffServ
Optimalizováno na vnitřní pokrytí	Optimalizováno na venkovní NLOS spojení
CSMA/CA - negarantuje QoS	Deterministický přístup k MAC
Nepodporuje MASH (dle nějakého standardu)	Podporuje MASH topologii
Dosah – stovky metrů	Dosah – desítky kilometrů (buňka typicky 7-10km)
Není zde problém „skrytého uzlu“	
Maximální „multi-path delay“ 0,8μs	Tolerantní k vícecestnému šíření signálu (až 10.0μs)

O zabezpečení se stará ve WiMAXu speciální podvrstva PS (Privacy Sub-layer)



Privacy Sub-layer poskytuje : řízení přístupu
šifrování datového spoje

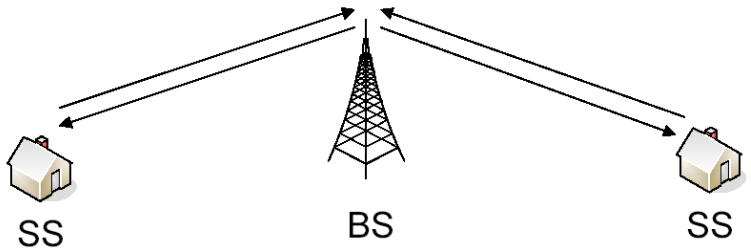
Autentizace je založena na certifikátech X.509 a stará se o ni podvrstva MCP (MAC Common Part Sublayer)

Bezpečnostní architektura IEEE 802.16 obsahuje pět základní částí:

- bezpečnostní asociace - SA
- certifikáty standardu X.509
- autentizace pomocí EAP-PKM
- správu klíčů
- šifrovací algoritmy (DES, AES)

Bezpečnostní model

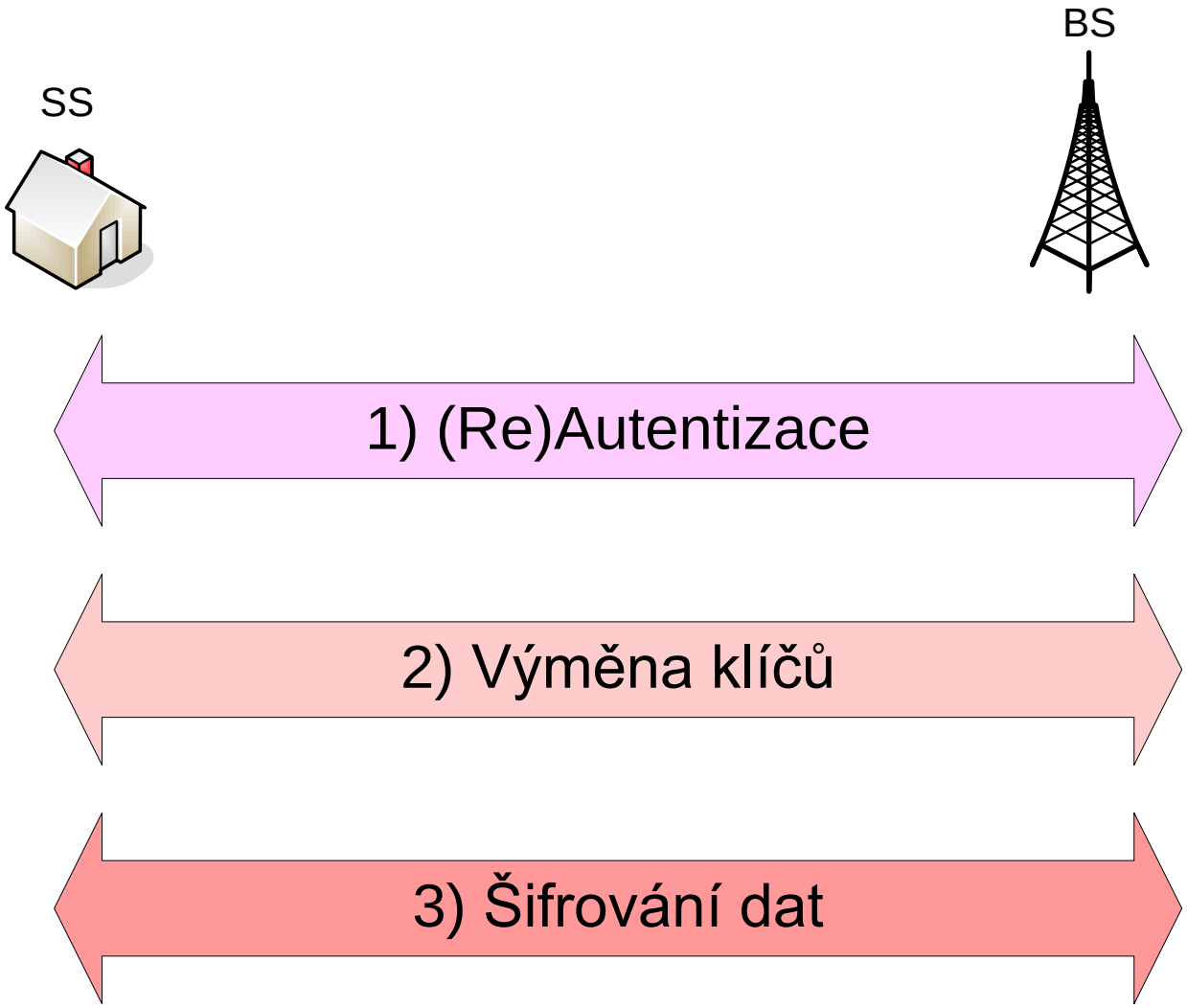
- Standard vychází ze specifikace DOCSIS (Data Over Cable Service Interface Specifications)
  - Předpoklad: Všechna zařízení (včetně přenosového média) jsou pod kontrolou poskytovatele.
  - Těžko splnitelné pro bezdrátové prostředí.
- Jednotlivá spojení v rámci BS jsou rozlišena pomocí bezpečnostních asociací (SA – Security Association).
- Bezpečnostní asociace obsahují bezpečnostní parametry (šifrovací algoritmy, hashovaní funkce, klíče, iniciační vektory..) související s konkrétním spojením.
- Standard 802.16-2004 explicitně definuje u SA pouze u datových spojení.
- Jednotlivé SA jsou rozlišeny pomocí SAID (SA Identifier).



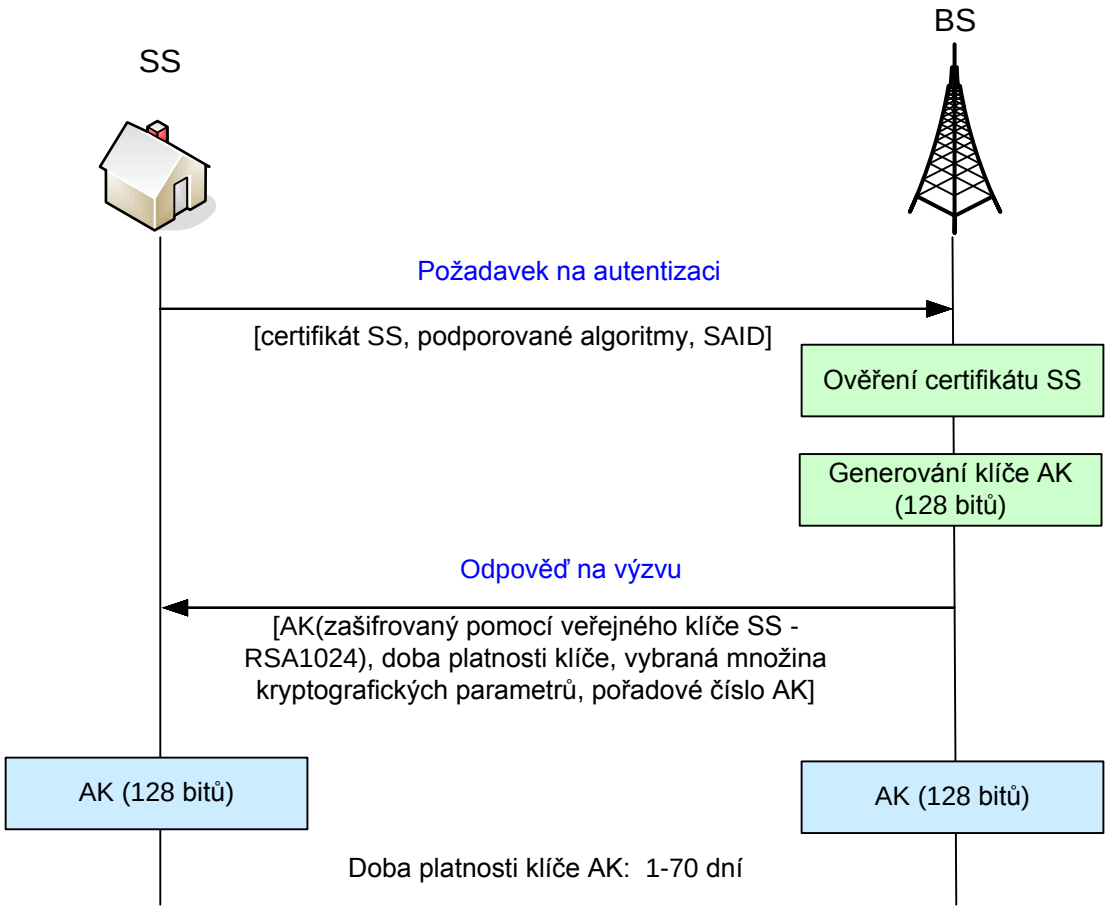
První verze 802.16 (až do 802.16:2004) vyžadovaly podporu pouze jediného šifrovací algoritmu - DES v režimu CBC
- chyběla podpora integrity (pouze CRC)
- snadno prolomitelné (podobná situace jako u WEPu v 802.11)

Od varianty IEEE 802.16e dále je povinně podporován
- algoritmus AES v režimu CCM (Counter CBC mode)
- kontrola integrity pomocí hashovací funkce SHA-1
- autentizace pomocí protokolu EAP-PKM
+ formální definice SA pro řídící rámce

WiMAX - průběh zabezpečení



Autentizace



SS →BS: Cert(Manufacturer(SS))

SS →BS: Cert(SS) | Capabilities | SAID

BS →SS: RSA-Encrypt(PubKey(SS), AK) | Lifetime | SAIDList | SeqNo

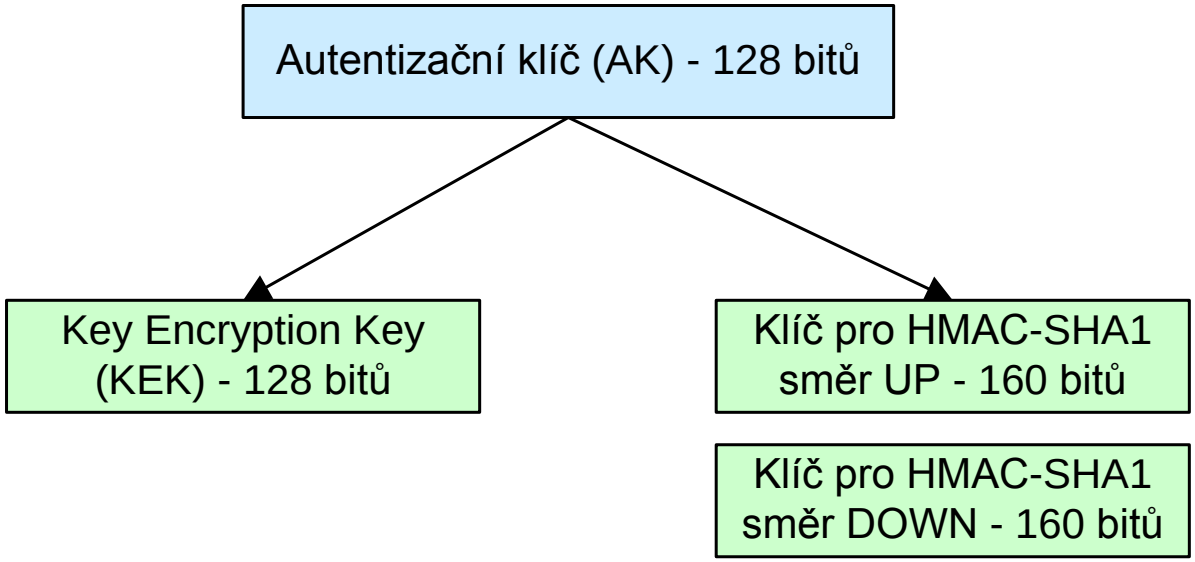
Autentizace - nevýhody

- AK je vygenerován na BS
- AK je vygenerován pouze z dat od BS
- SS se na „výrobě“ AK nijak nepodílí
- SS musí důvěřovat AK, že klíč vygenerován korektně
- Lepší řešení – generování AK z dat od SS i BS

(jako u SSL – Client Random, Server Random)

- Autentizace je pouze jednosměrná (SS->BS)
- Chybí autentizace BS vůči SS – možnost existence falešných BS

Odvození klíčů

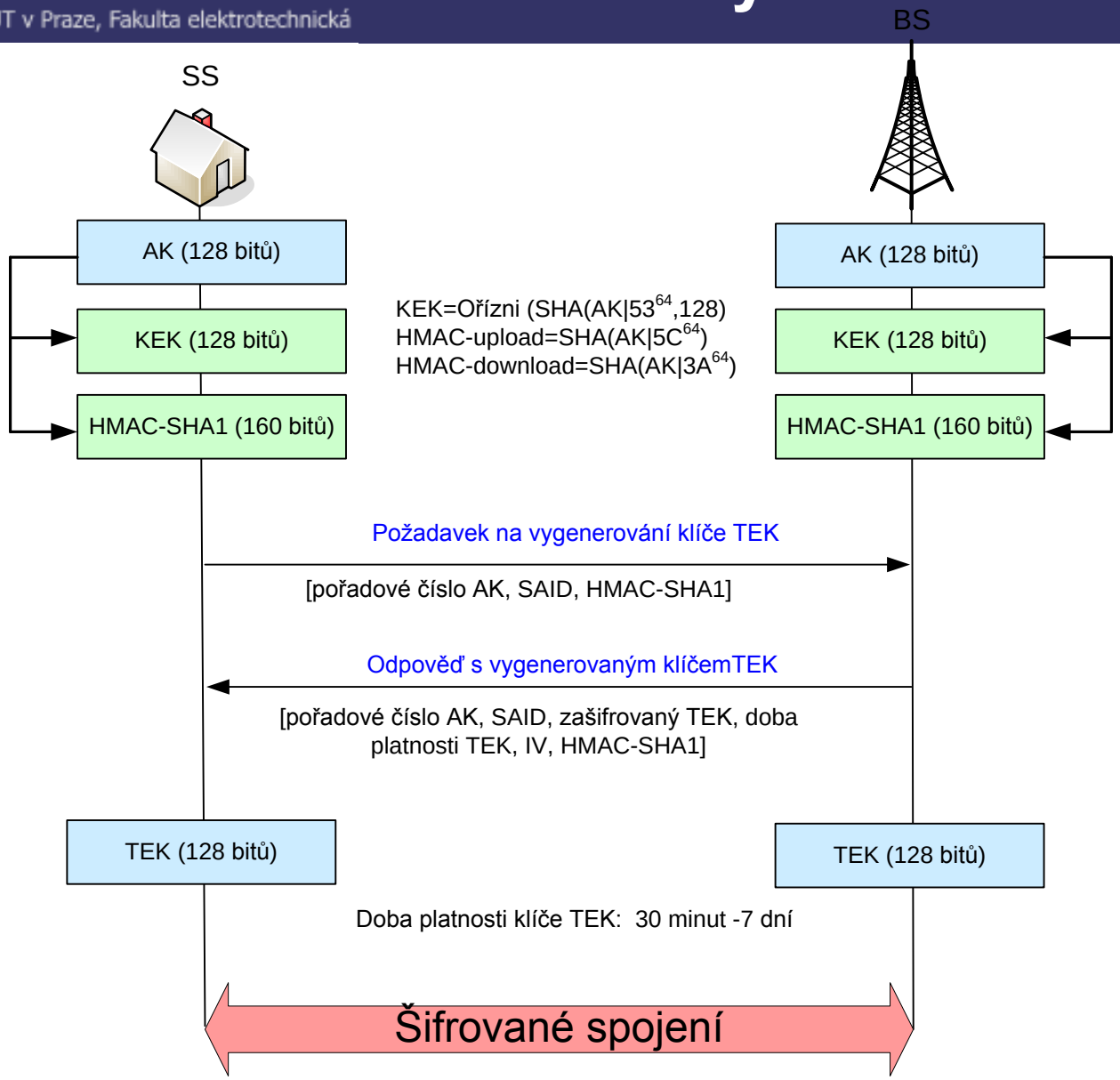


KEK = Truncate-128(SHA1(((AK| 0^{44}) xor 53^{64})

Klíč pro Downlink HMAC-SHA1 = SHA1((AK|0^{44}) xor $3A^{64}$)

Klíč pro Uplink HMAC-SHA1 = SHA1((AK|0^{44}) xor $5C^{64}$)

Výměna klíčů



Obnova klíčů

1) *BS* →*SS*: *SeqNo* | *SAID* | *HMAC*(1)

2) *SS* →*BS*: *SeqNo* | *SAID* | *HMAC*(2)

3) *BS* →*SS*: *SeqNo* | *SAID* | *OldTEK* |*NewTEK* | *HMAC*(3)

TEK: zašifrován pomocí 3DES-ECB

Výměna klíčů

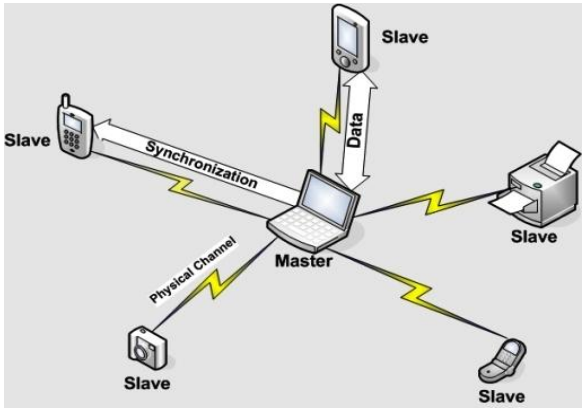
- TEK - Traffic Encryption Key
- BS vygeneruje náhodný TEK
- TEK je zašifrován pomocí algoritmu
  - 3DES-EDE2 (klíčem je klíč KEK o délce 128bitů)
  - RSA (modul délky 1024b, veřejný exponent $e=2^{16}+1$)
  - AES-128-ECB (klíčem je klíč KEK o délce 128bitů)
- Výměna klíčů je autentizována pomocí HMAC-SHA1 – (zajišťuje také integritu a potvrzení AK)

Praxe:

- Šifrovány jsou pouze datové zprávy
- Řídící rámce jsou nešifrované (802.16:2004)
- Implementován je pouze povinný je pouze DES v režimu CBC
  - 56 bitový klíč DES (TEK)
  - Žádná metoda zajištění integrity
  - Žádná ochrana proti Replay útokům

Bluetooth

- 2002 – IEEE 802.15.1.
- ISM pásmo - 2.4GHz
- NLOS rádiová technologie pro PAN
- dosah řádově metry/desítky metrů
- přenosová rychlost – řádově jednotky Mbit/s
- PICONET – jedno zařízení typu „master“ může komunikovat až ze sedmi zařízeními typu „slave“



Bluetooth

Základní bezpečnostní komponenty

- FH - frequency hopping
  - přeskakování mezi kmitočty
- jedinečná adresa zařízení
  - BD_ADDR
  - 48 bitů
- klíče odvozené z PIN
  - 128 bitů
- autentizace zařízení sdíleným 128bitovým klíčem
- utajení dat zajištěno proudovou šifrou s konfigurovatelnou délkou klíče (8-128 bitů)

IEEE 802.15

Bezpečnostní algoritmy v Bluetooth

- E0 – šifrování přenášených dat (komunikace)
  - viz . přednáška
- E1 – autentizace
- E21 – generování klíčů
- E22 – generování inicializačního klíče
- E3 – generování šifrovacího klíče
- Komunikace dvou uzlů, které se nalezly začíná dojednáním klíče pro šifrování radiového spoje (linky)
- Kritická fáze komunikace – z inicializačního klíče se generuje klíč linky pro šifrování rádiového spoje
- v BT se autentizují zařízení (ne uživatelů)

BT - autentizace

- používá se linkový klíč
  - získá se jako buď jako klíč zařízení, kombinační klíč, nebo hlavní klíč

  1) Klíč zařízení (unit key) se generuje při instalaci zařízení. Nemění se při komunikaci s různými zařízeními.

  2) Kombinační klíč (combination key) se po dohodě generuje ve fázi inicializace kombinací klíčů komunikujícího páru stanic. Je bezpečnější než použití klíče zařízení, který je stejný pro jakoukoli komunikaci daného zařízení.

  3) Klíč spoje - bud' trvalý (uložený v paměti nezávislé na napájení) nebo dočasný.
- Účastníci musí sdílet jeden hlavní klíč (master key), který nahrazuje jednotlivé klíče spoje.
- autentizace používá princip výzva-odpověď

BT - autentizace

- Vyzyvatel zašle svoji adresu a od druhé komunikující strany dostane náhodné číslo.
- Na základě těchto hodnot a sdíleného klíče spoje se pomocí autentizační funkce spočítá výsledek, který si obě strany porovnají.
- autentizace jednostranná nebo vzájemná
  - standard to neřeší
  - cílem je ve dvou krocích ověřit, zda druhá strana zná sdílený klíč.
- autentizaci lze provést automaticky bez interakce s uživatelem

Fáze procesu zabezpečení u BT

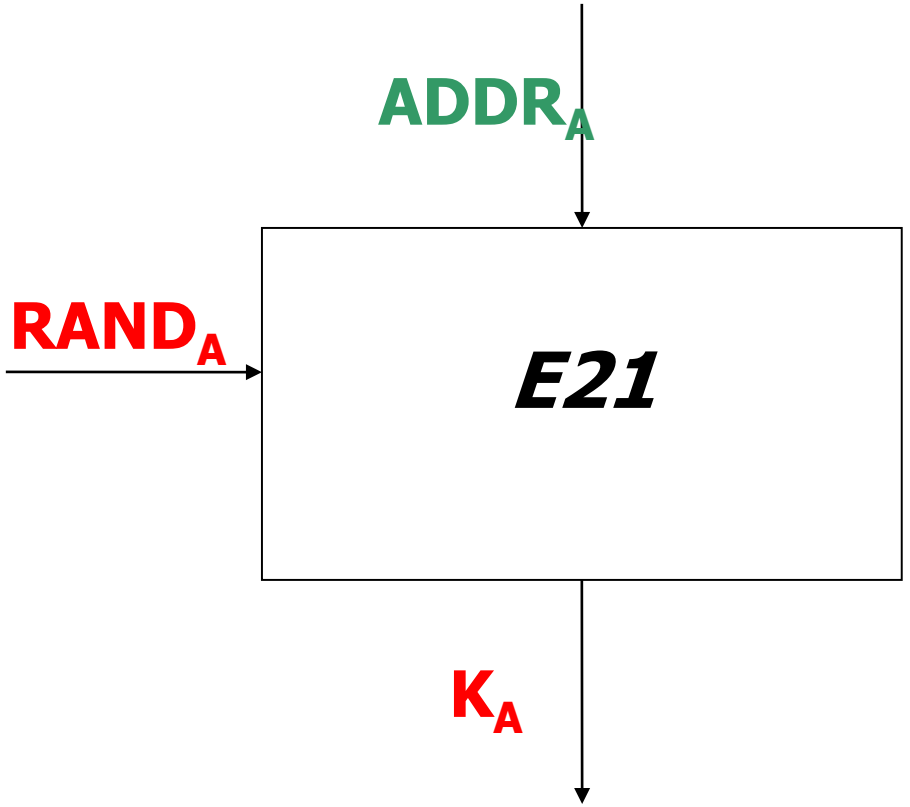
- Generování klíče zařízení
- Generování inicializačního klíče
- Generování linkového klíče
- Vzájemná autentizace
- Generování šifrovacího klíče
- Generování proudu klíče
- Šifrování dat

Fáze procesu zabezpečení u BT

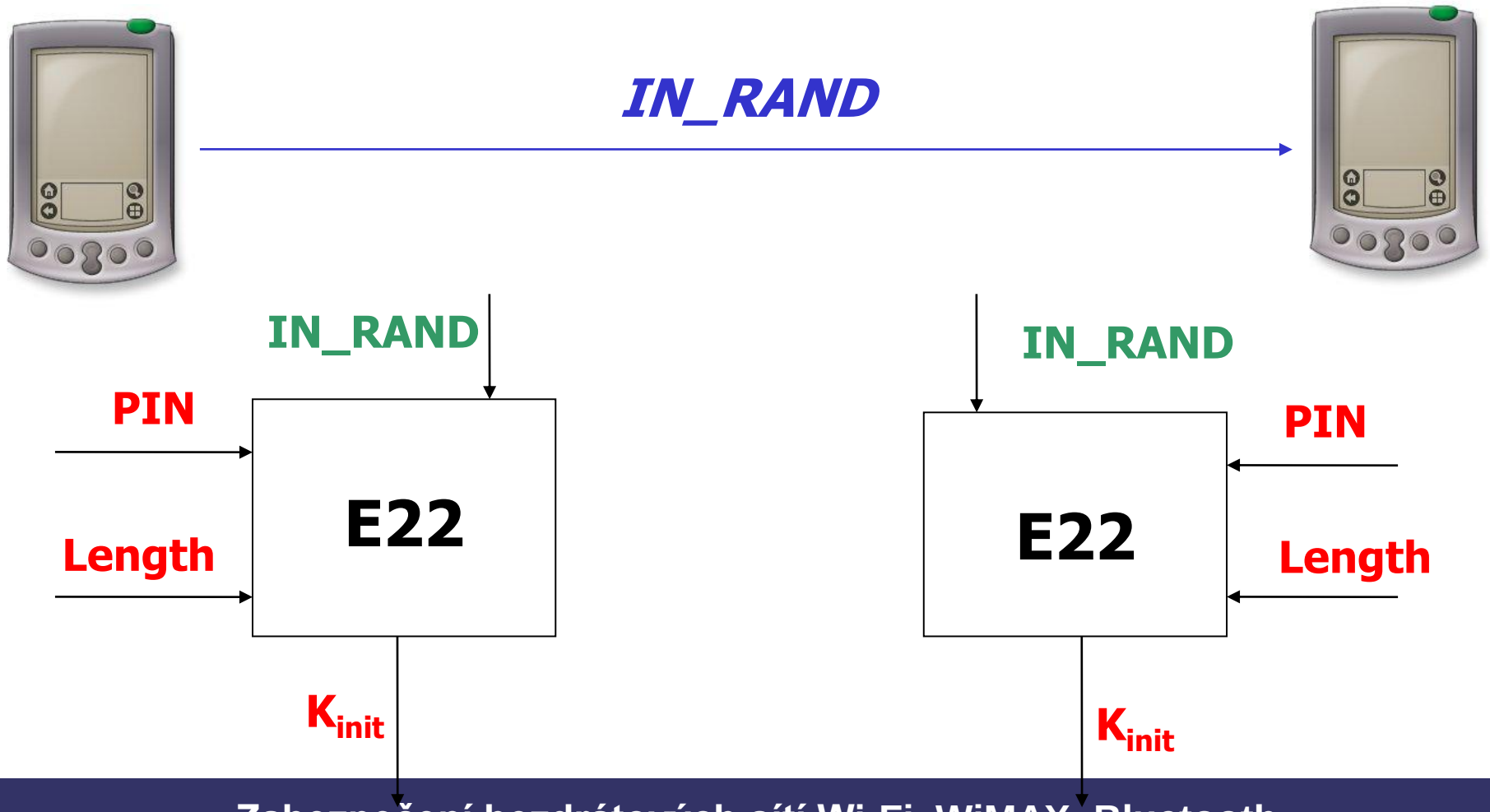
XXX = veřejná hodnota (není nutné ji tajit)
XXX = tajná hodnota (informace)

XXX = zpráva odeslaná v OT
XXX = zpráva odeslaná v ŠT

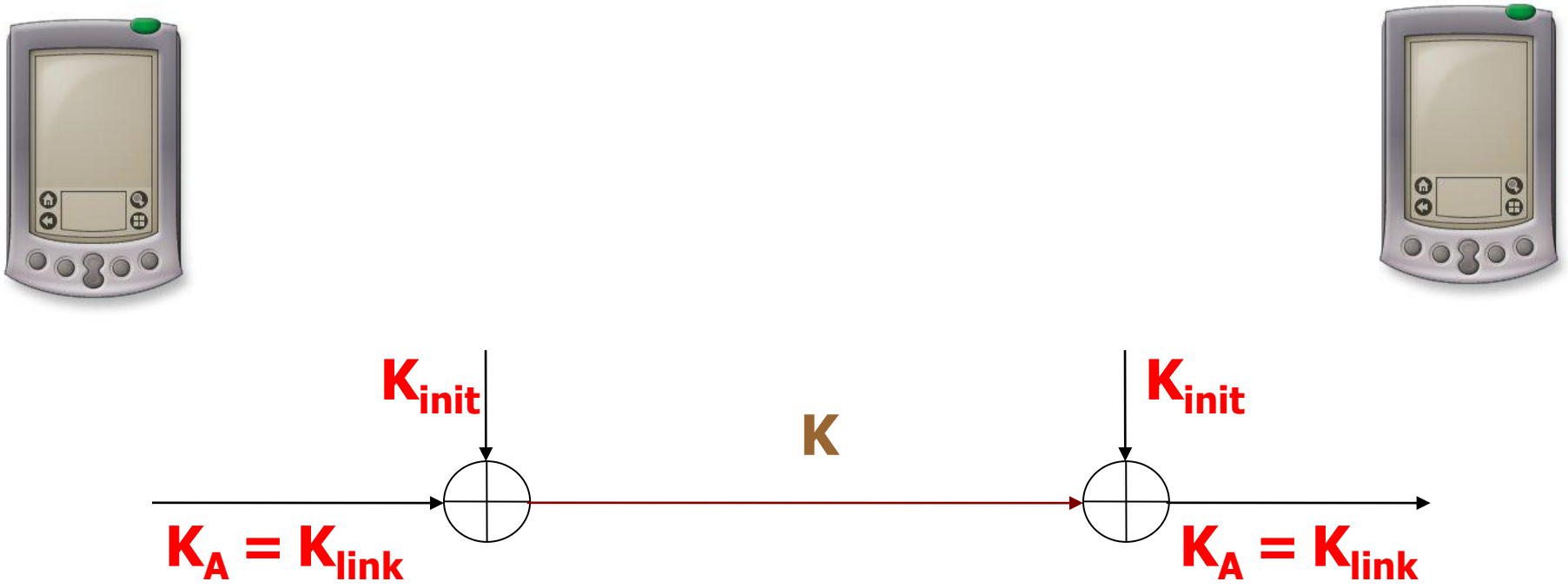
1. Generování klíče jednotky (unit key)



2. Generování inicializačního klíče

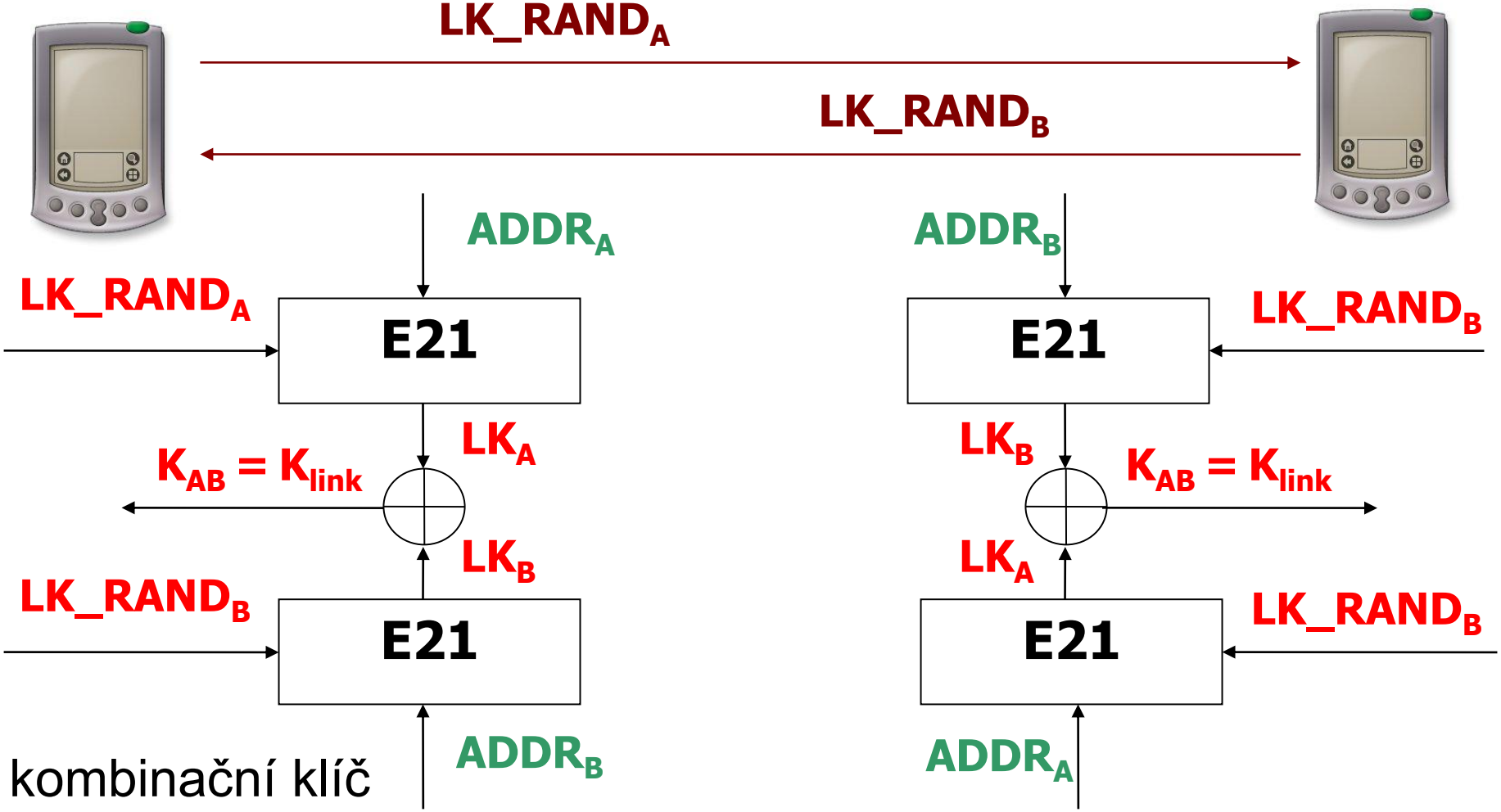


3. Generování linkového klíče (1)



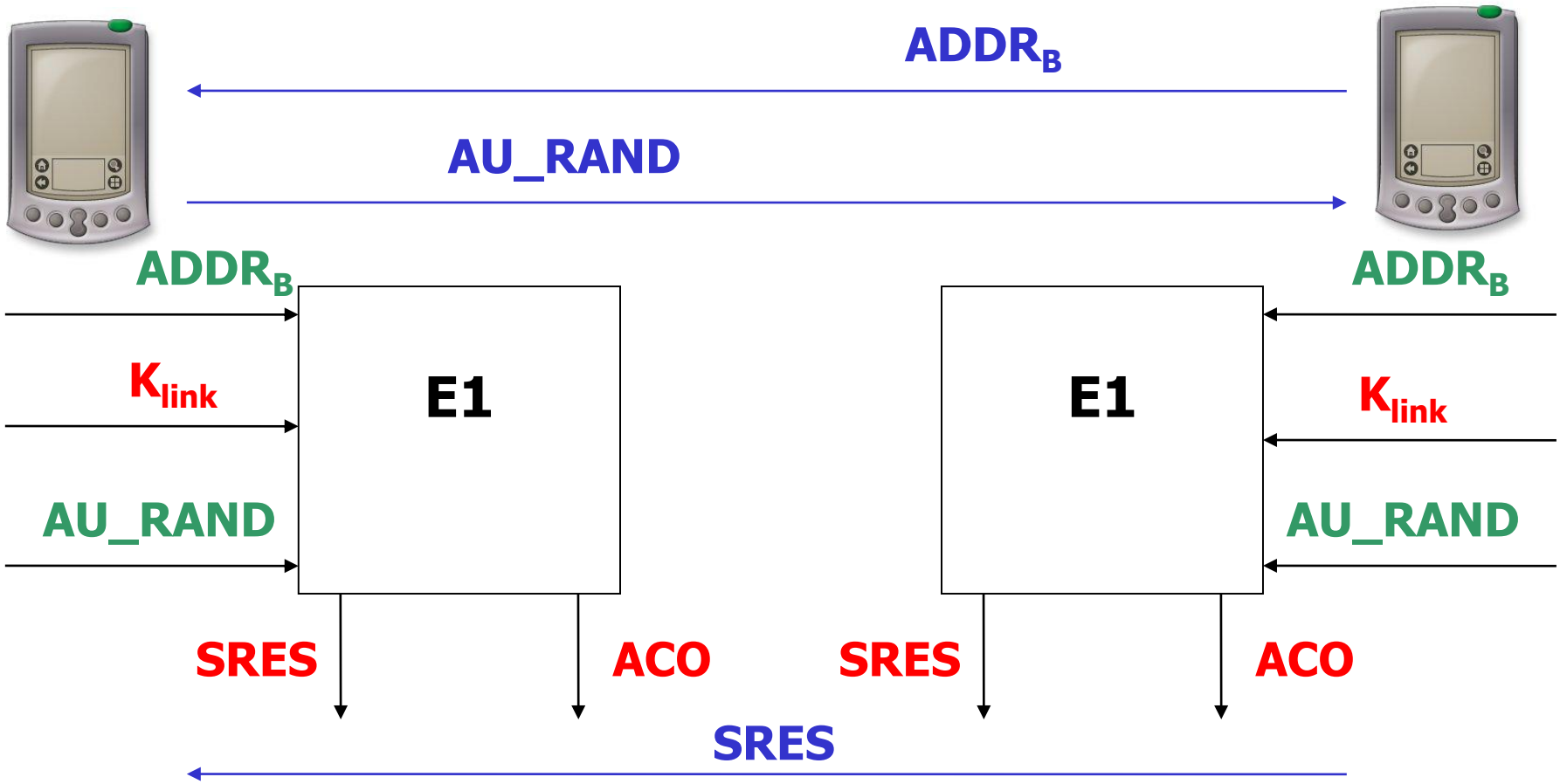
- generování z klíče jednotky vyzyvatele

3. Generování linkového klíče (2)

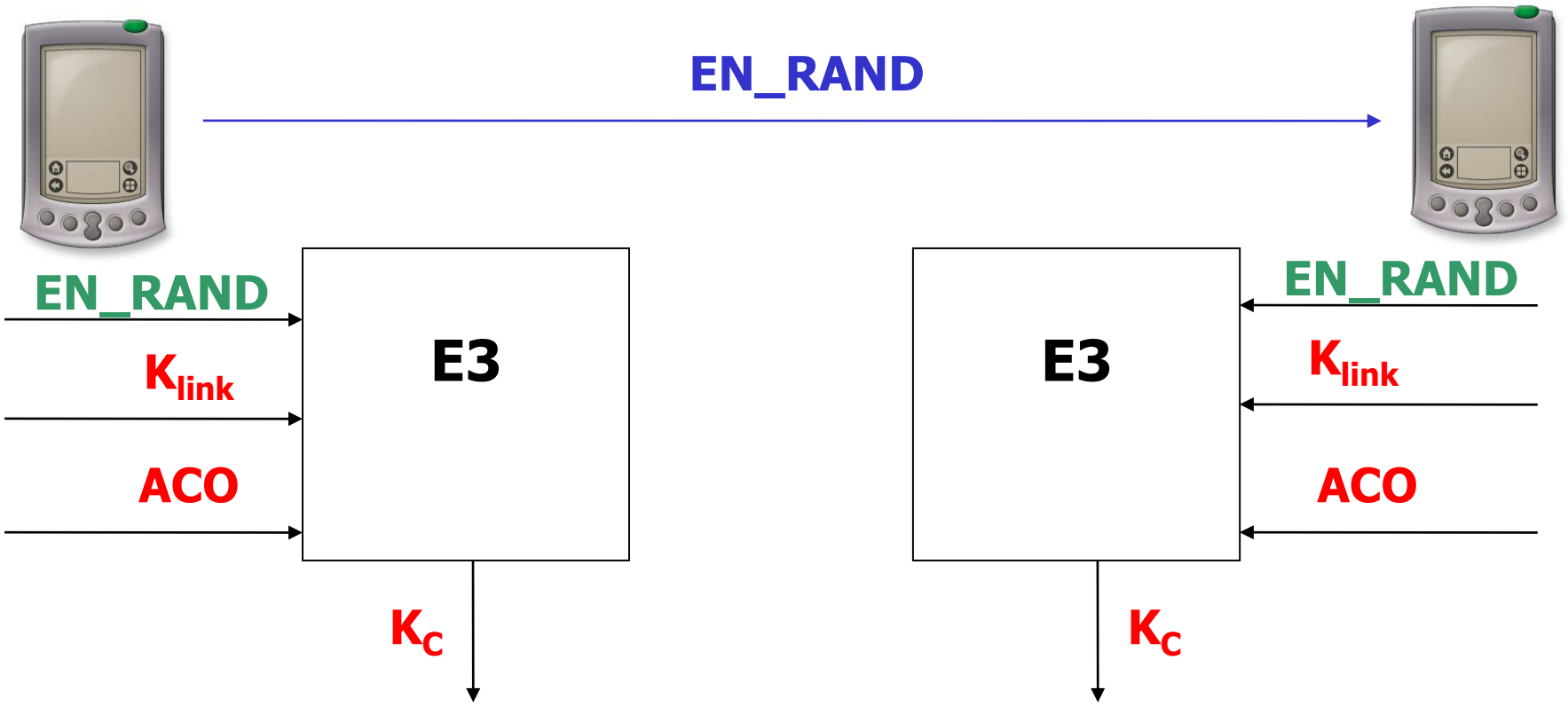


- kombinační klíč

4. Vzájemná autentizace zařízení

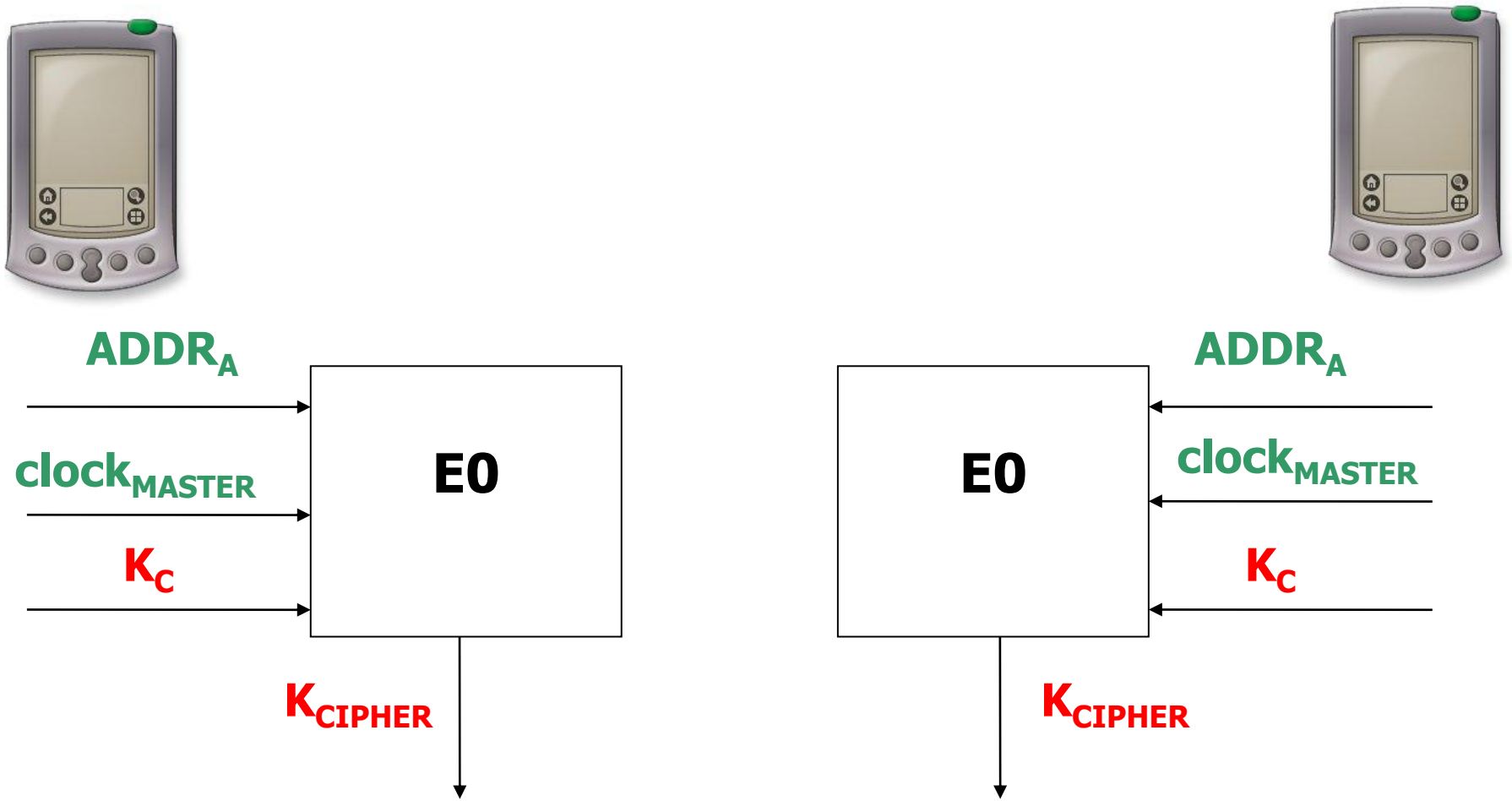


5. Generování šifrovacího klíče



ACO (Authenticated Ciphering Offset)

6. Generování proudu klíče



7. Šifrování přenášených dat