LABKA.CZ
HACKERSPACE
OSTRAVA

LABKA.CZ
HACKERSPACE
OSTRAVA

LABKA KRYPTOSYSTÉMY

AUTOR: ADAM LICHNOVSKÝ

DATUM: 3.5.2017

LABKA.CZ
HACKERSPACE
OSTRAVA

OBSAH

- Úvod
- Kryptografické systémy
- Obecný návrh kryptografického systému
- Public key infrastructure (PKI)
- Ukázka komunikace pomocí obecného kryptografického systému
- Ukázka komunikace pomocí TLS_RSA_WITH_AES_128_CBC_SHA256

ÚVOD

- ÚVODNÍ SLOVO
- UJASNĚNÍ POJMŮ
- RÁMEC PŘEDNÁŠKY
- "AUTOR BY SI PŘÁL, ABY TOTO POJEDNÁNÍ PŘISPĚLO K ODSTRANĚNÍ MNOHÝCH PŘEDSUDKŮ NA JEDNÉ STRANĚ A MNOHÝCH POVRCHNÍCH A PLYTKÝCH ŘEČÍ NA STRANĚ DRUHÉ."
  – *MNICHOV, 31.3. 1809, F.W.J. SCHELLING*

KRYPTOGRAFICKÉ SYSTÉMY

KRYPTOGRAFICKÉ SYSTÉMY

- V KRYPTOGRAFII KRYPTOGRAFICKÝMI SYSTÉMY MYSLÍME BALÍKY KRYPTOGRAFICKÝCH ALGORITMŮ, KTERÉ POTŘEBUJETE PRO IMPLEMENTACI KONKRÉTNÍ BEZPEČNOSTNÍ SLUŽBY. NEJČASTĚJI K ZAJIŠTĚNÍ DŮVĚRNOSTI A AUTENTIČNOSTI POSÍLANÉ ZPRÁVY (ZAŠIFROVÁNO A ZAPEČETĚNO).
- BĚŽNĚ SE KRYPTOSYSTÉMY SKLÁDAJÍ ZE TŘÍ ALGORITMŮ:
  - ALGORITMUS PRO GENEROVANÍ KLÍČŮ,
  - ALGORITMUS PRO ZAŠIFROVÁNÍ,
  - ALGORITMUS PRO ODŠIFROVÁNÍ.

- TERMÍN ŠIFRA(CIPHER, CYPHER) ČASTO OZNAČUJE PÁR ALGORITMŮ,
  - ALGORITMUS PRO ZAŠIFROVÁNÍ,
  - ALGORITMUS PRO ODŠIFROVÁNÍ.

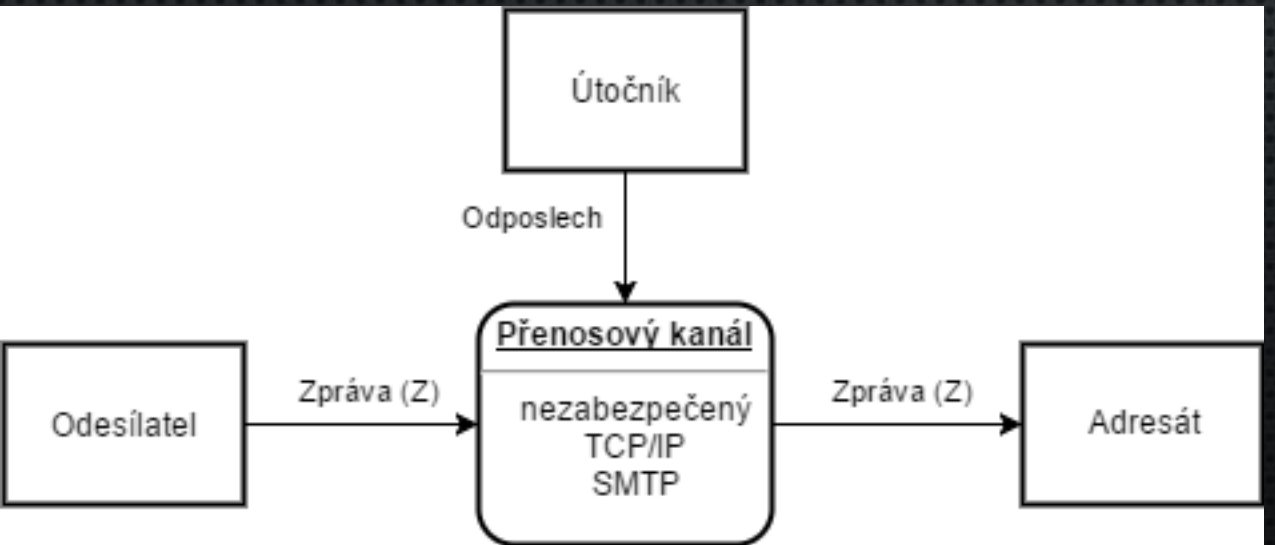
KRYPTOGRAFICKÉ SYSTÉMY

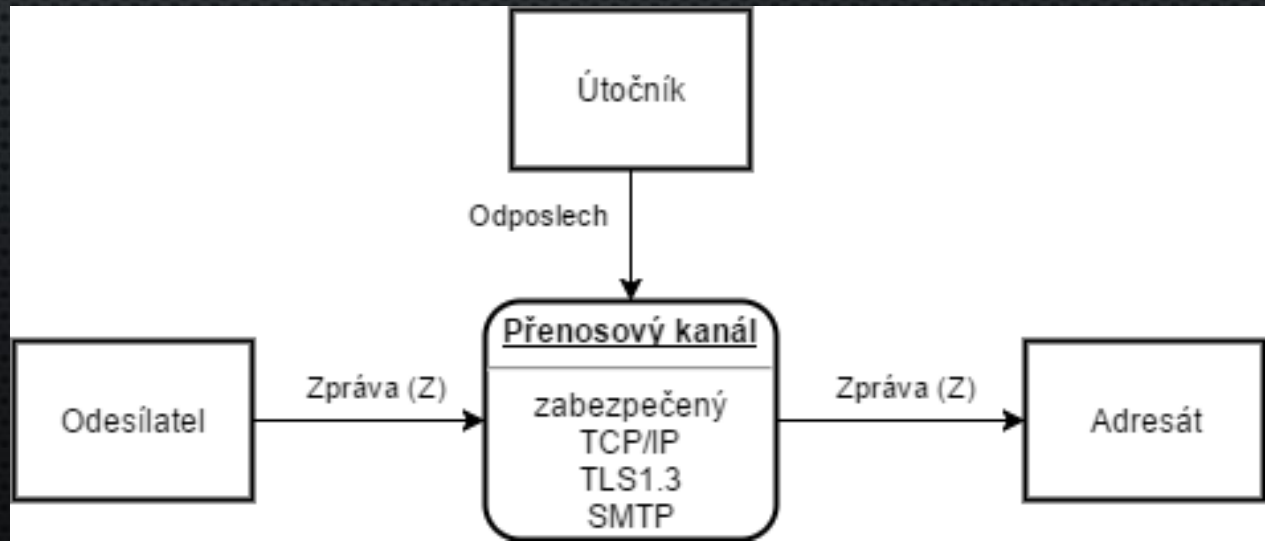
ŠIFRY

- ŠIFRA JE JAKÁKOLIV METODA ZAŠIFROVÁNÍ TEXTU PŘI ZACHOVÁNÍ ČITELNOSTI A VÝZNAMU. ČASTO SE ŠIFROU OZNAČUJE ZAŠIFROVANÝ TEXT ZPRÁVY, PŘESTO DÁLE BUDEME PREFEROVAT OZNAČENÍ KRYPTOGRAM.

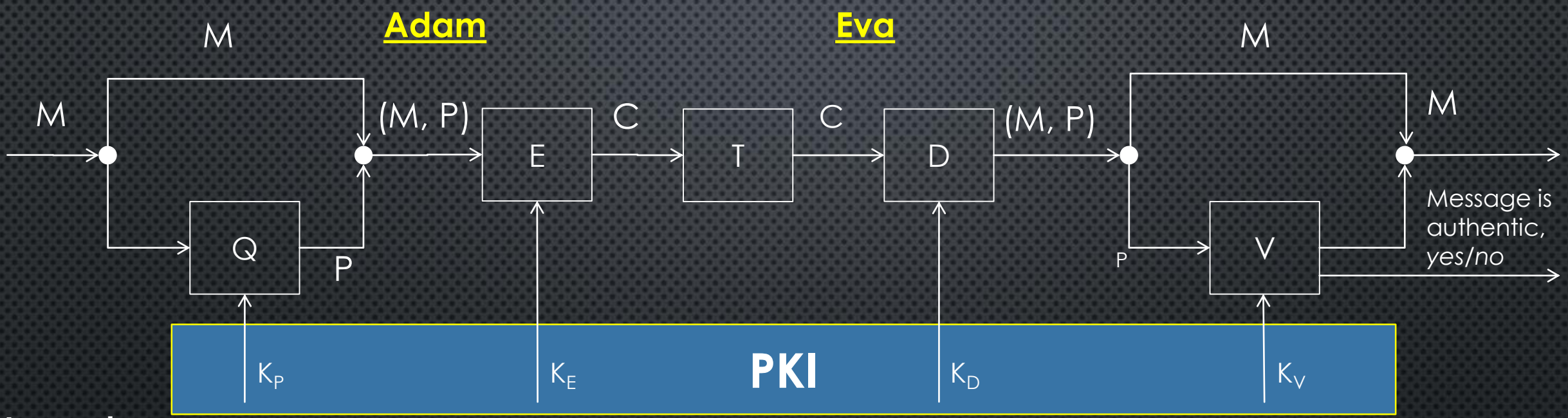
KRYPTOGRAM

- ZAŠIFROVANÝ TEXT ZPRÁVY





OBECNÝ NÁVRH KRYPTOGRAFICKÉHO SYSTÉMU



Legend:

M – Zpráva
Q – Pečetící (Podpisový) stroj
E – Šifrovací stroj
P – Pečeť (Podpis)
C – kryptogram s pečetí (M, P)
T – Přenosový stroj
D – Dešifrovací stroj
V – Ověřovací stroj

$\mathbf{K_P}$ – Pečetící klíč (Privátní klíč Adama)
$\mathbf{K_E}$ – Šifrovací klíč (Privátní klíč Adama)
$\mathbf{K_D}$ – Dešifrovací klíč (Veřejný klíč Adama)
$\mathbf{K_V}$ – Ověřovací klíč (Veřejný klíč Adama)
PKI – Public Key Infrastructure

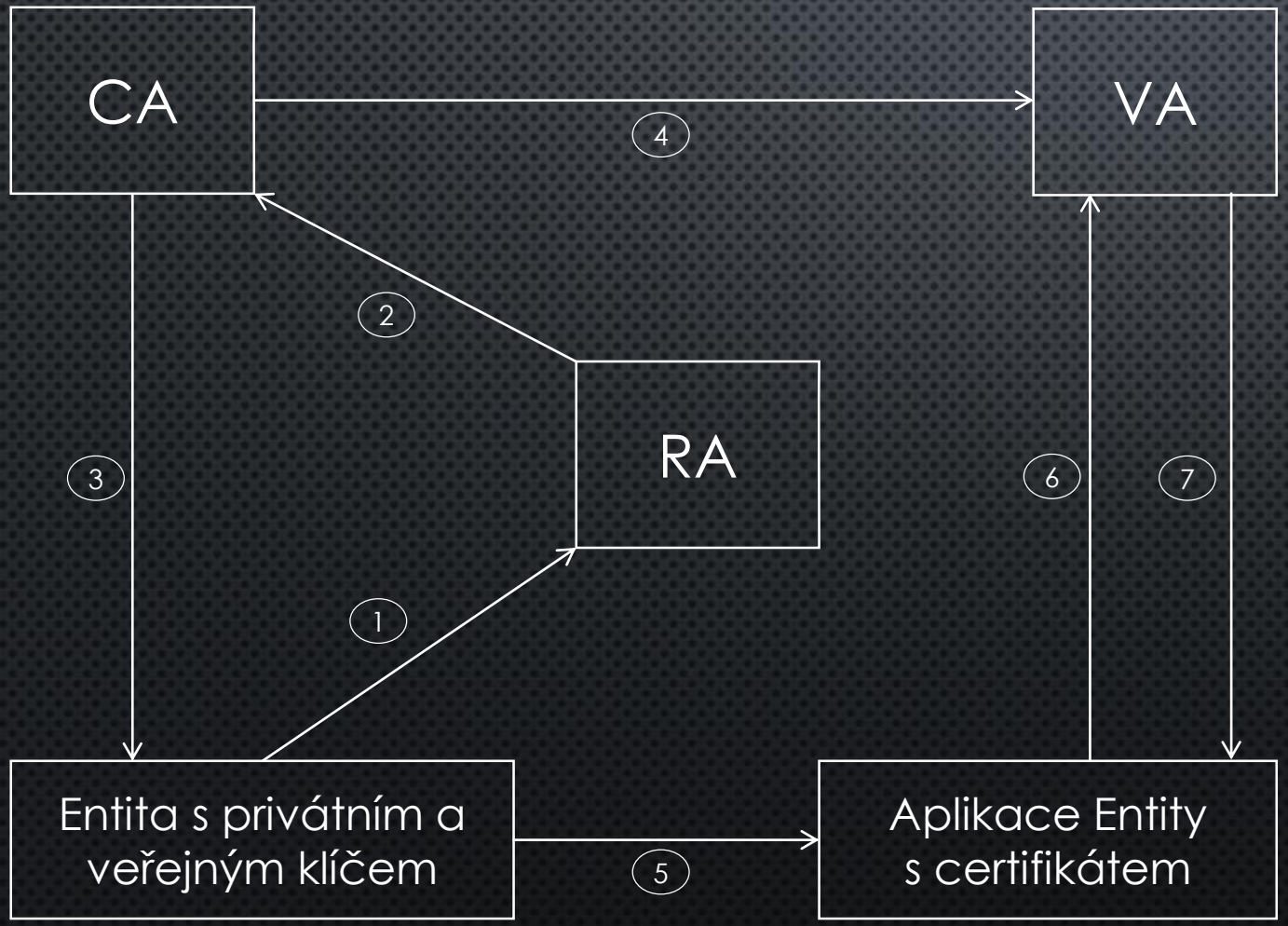
PUBLIC KEY INSTRASTRUCTURE (PKI)

- Public Key Infrastructure (PKI) – je systém pro tvorbu, ukládání a distribuci certifikátů, které jsou používané k ověření, zda konkrétní veřejný klíč patřící adekvátní entitě (uživatel, server, aplikace). PKI vytváří digitální certifikáty, ve kterých se mapuje veřejný klíč s entitou, následně certifikát uloží v centrálním repositáři. Pokud je potřeba je certifikát zrušen a odstraněn z repositáře.

PKI :

- CA – Certifikační autorita vydává a ověřuje digitalní certifikáty
- RA – Registrační autorita ověřuje identitu entity požadující informace od CA
- VA – Validační autorita ověřuje platnost vydaných certifikátů
- CD – Central directory—zabezpečené úložiště pro ukládání a indexaci certifikátů
- CMS – Certificate management system
- CP – Certificate Policy

PUBLIC KEY INSTRASTRUCTURE (PKI)

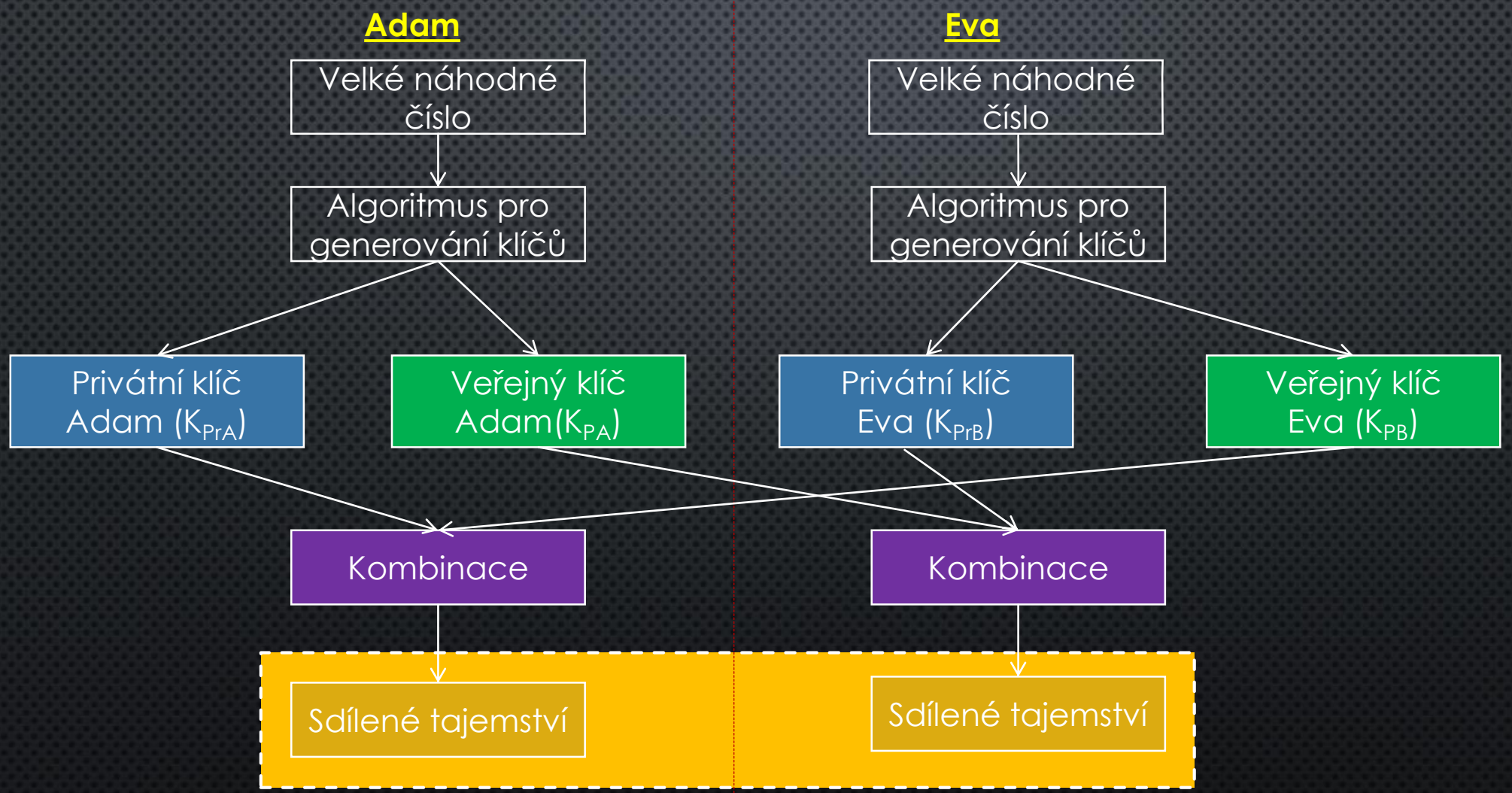


Certifikační a ověřovací proces

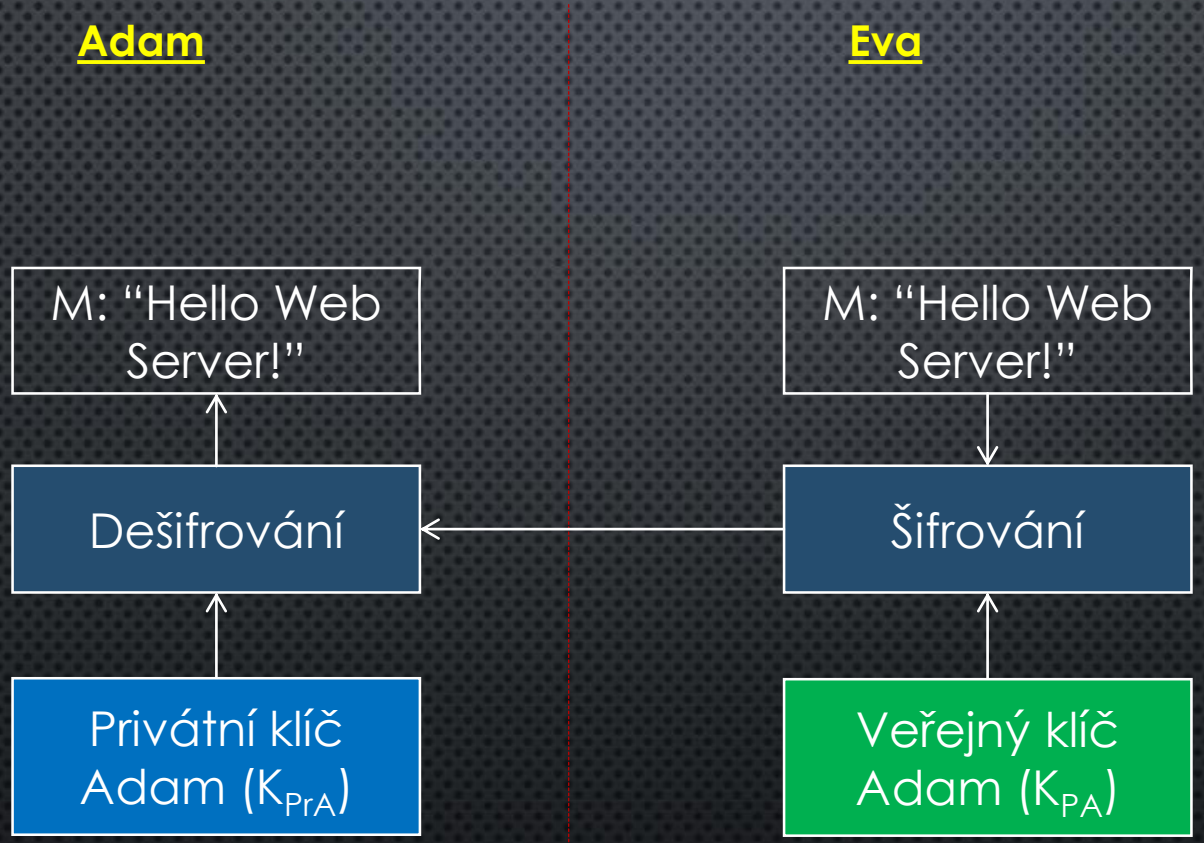
Kroky:

1. Entita požádá o vydání certifikátu od RA
2. RA schválí nebo zamítnou certifikační požadavek, a pokud RA schválí certifikační požadavek, pak RA požádá CA o vydání certifikátu pro Entitu.
3. CA vydá certifikát pro Entitu
4. CA aktualizuje centrální úložiště a certifikační revokační list (CRL) pro VA
5. Entity přidá certifikát do úložiště aplikace
6. Aplikace Entity požádá o ověření platnosti certifikátu
7. VA kdykoliv ověří platnost certifikátu Aplikace Entity podle CRL

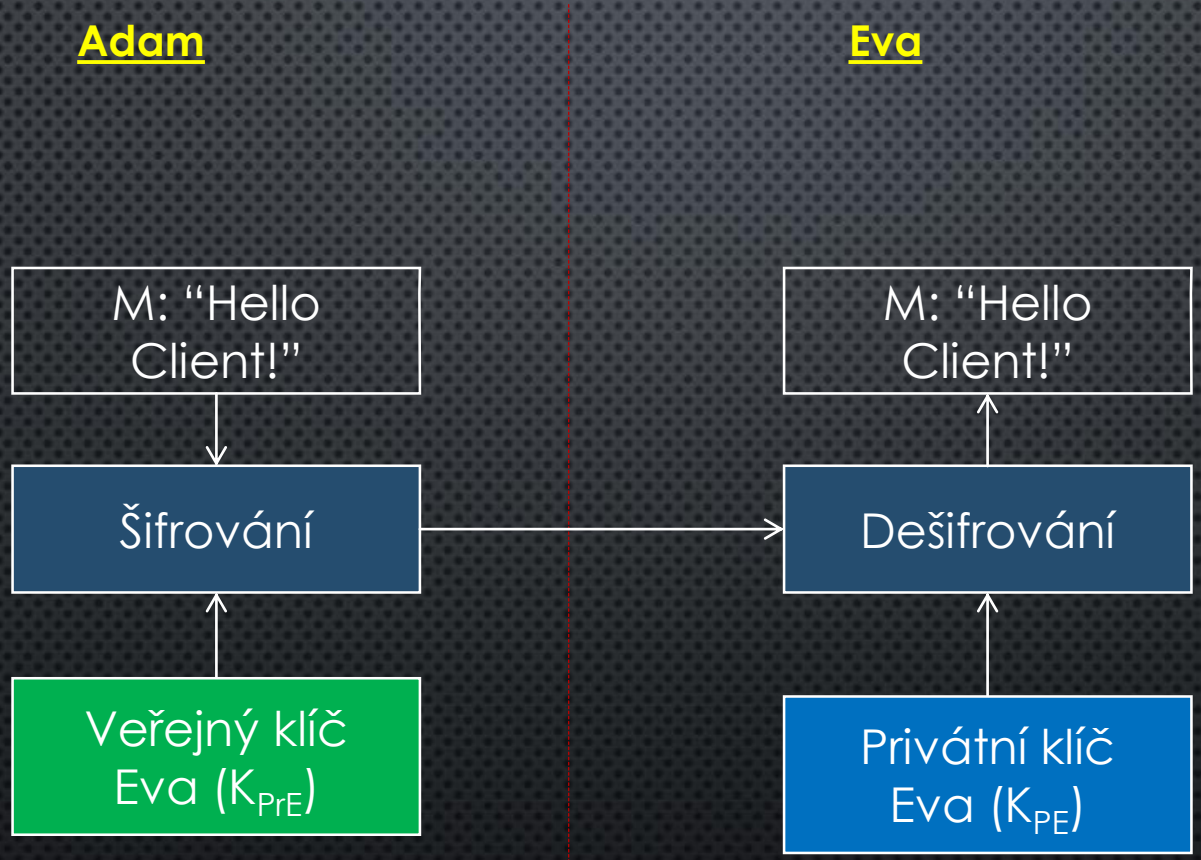
OBECNÝ KRYPTOGRAFICKÝ SYSTÉM



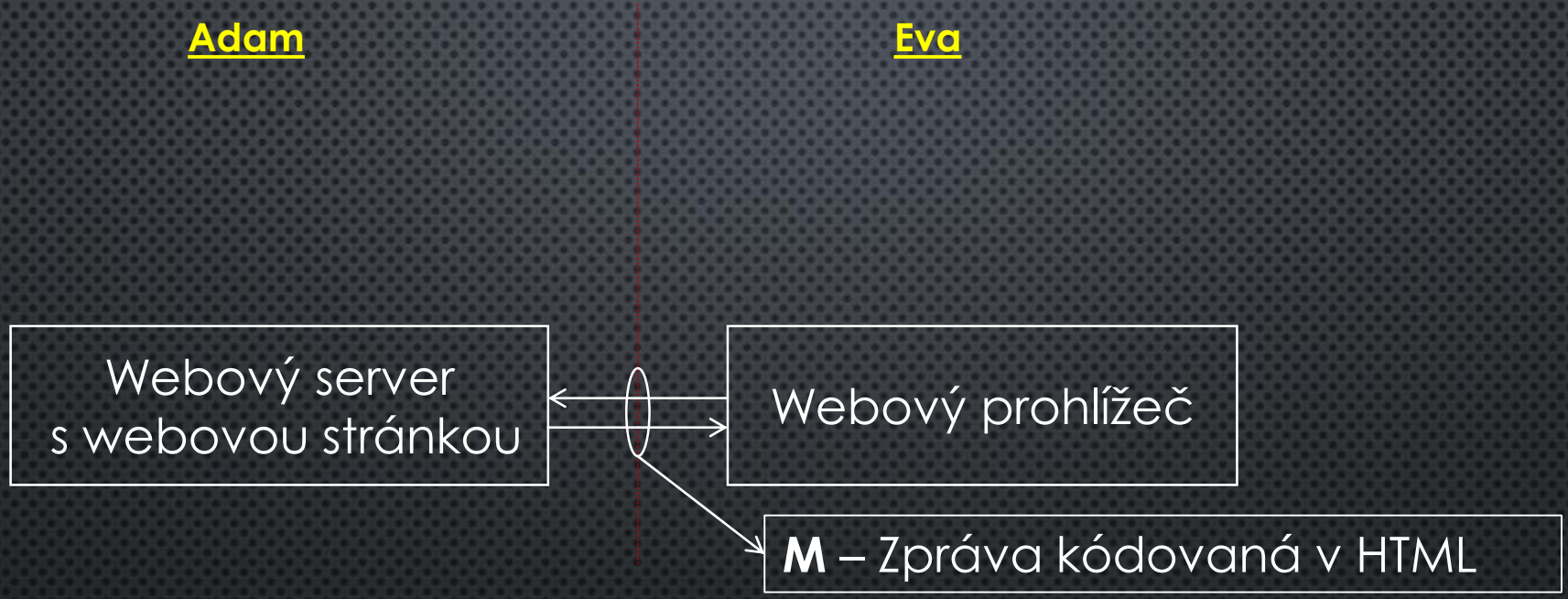
OBECNÝ KRYPTOGRAFICKÝ SYSTÉM



OBECNÝ KRYPTOGRAFICKÝ SYSTÉM



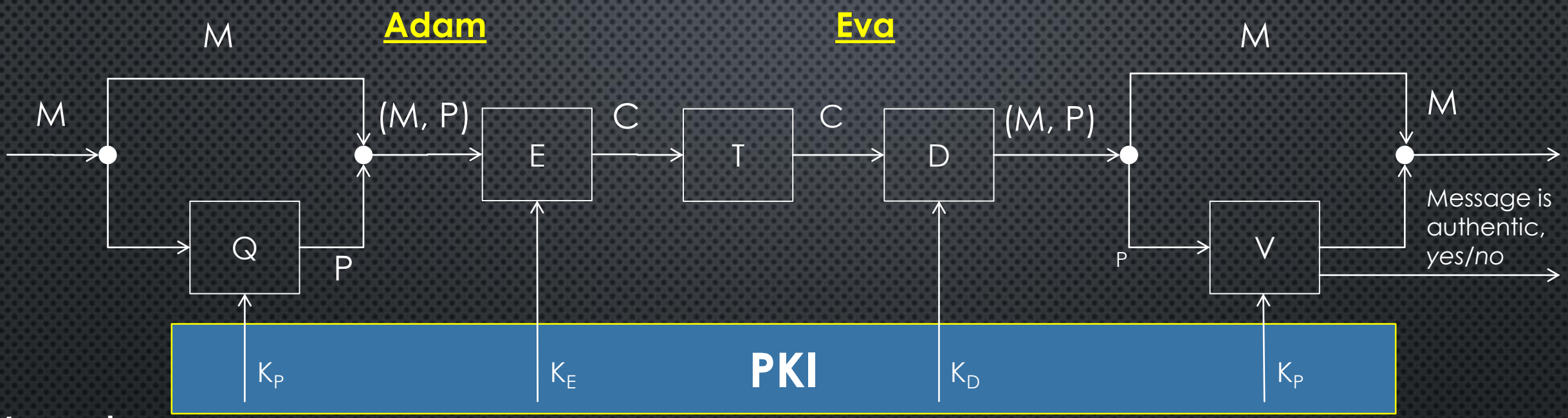
PŘÍKLAD TLS_RSA_WITH_AES_128_CBC_SHA256



Příklad:

Eva chce navštívit svou oblíbenou stránku svým oblíbeným webový prohlížečem. Webová stránka je hostována na webovém serveru u Adama, který podporuje pouze šifrovací balík TLS_RSA_WITH_AES_128_CBC_SHA256

PŘÍKLAD TLS_RSA_WITH_AES_128_CBC_SHA256

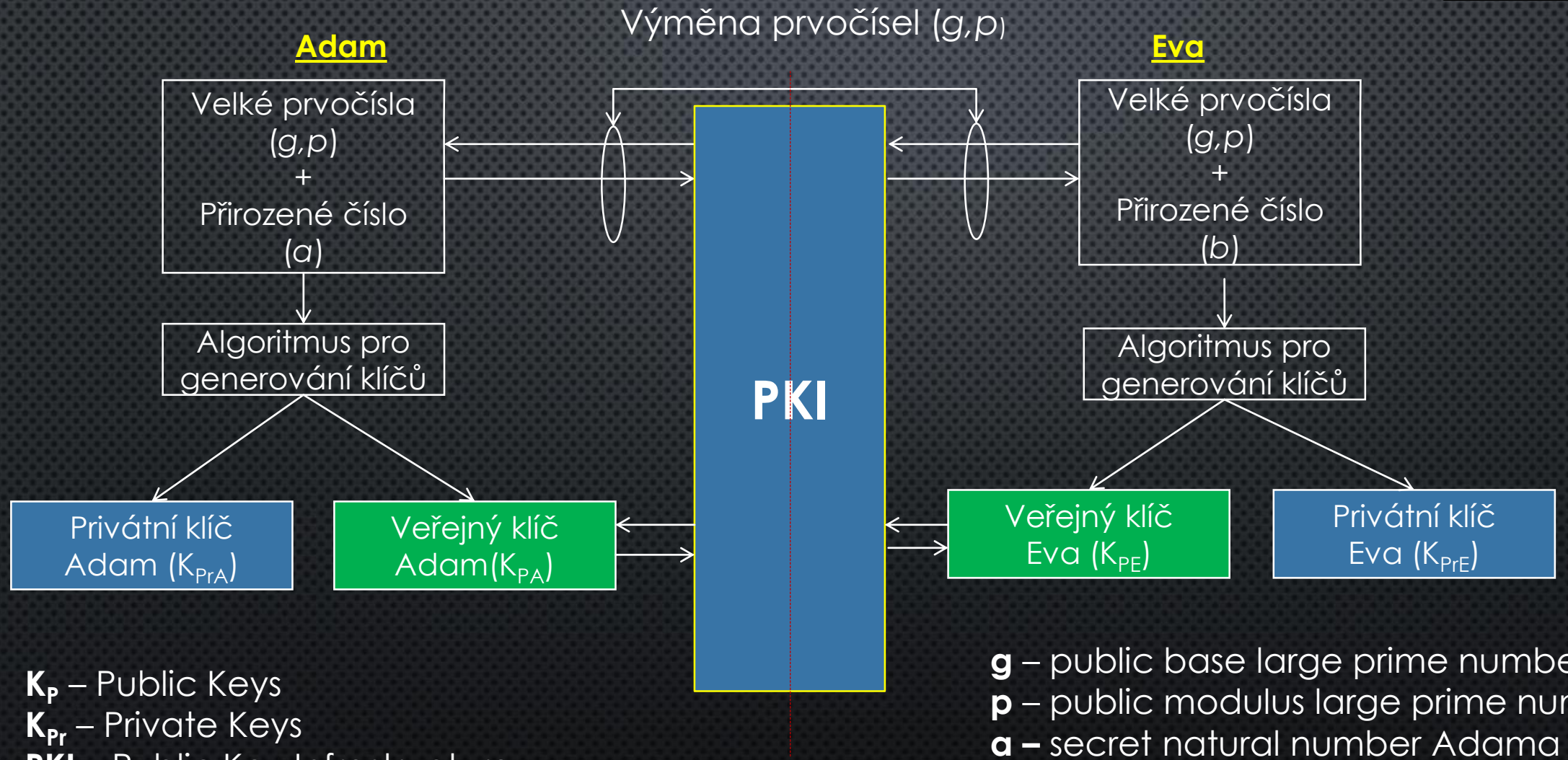


Legend:

M – Zpráva → HTML in HTTP
Q – Pečetící (Podpisový) stroj → SHA-256
E – Šifrovací stroj → CBC
P – Pečeť (Podpis)
C – Kryptogram s pečetí (M, P)
T – Přenosový stroj → RSA s AES-128 přes TCP/IP
D – Dešifrovací stroj → CBC
V – Ověřovací stroj → SHA-256

K_P – Pečetící klíč (Privátní klíč Adama)
K_E – Šifrovací klíč (Privátní klíč Adama)
K_D – Dešifrovací klíč (Veřejný klíč Adama)
K_V – Ověřovací klíč (Veřejný klíč Adama
PKI – Public Key Infrastructure

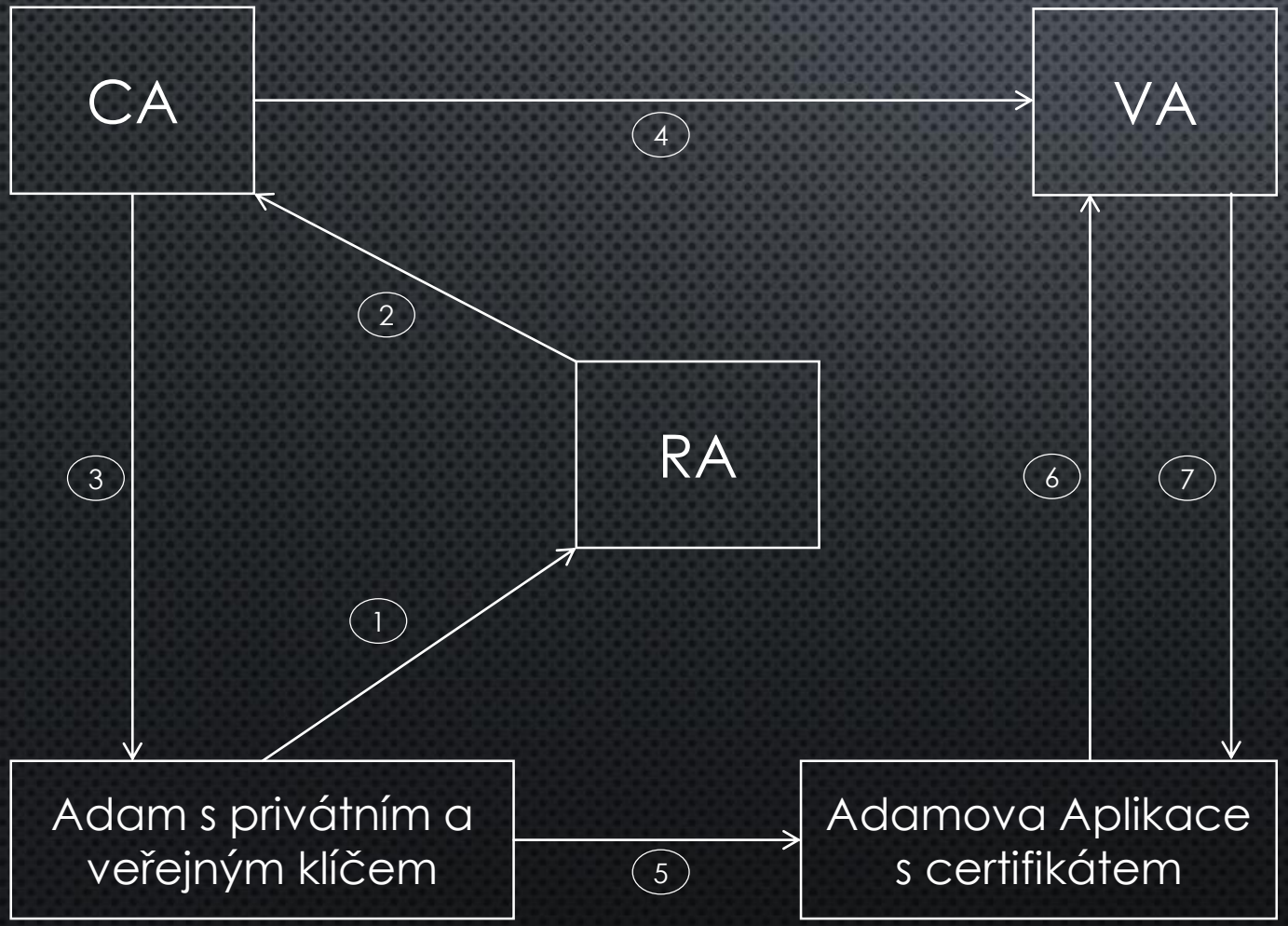
PŘÍKLAD TLS_RSA_WITH_AES_128_CBC_SHA256



K_P – Public Keys
K_{Pr} – Private Keys
PKI – Public Key Infrastructure

g – public base large prime number
p – public modulus large prime number
a – secret natural number Adama
b – secret natural number Evy

PŘÍKLAD TLS_RSA_WITH_AES_128_CBC_SHA256

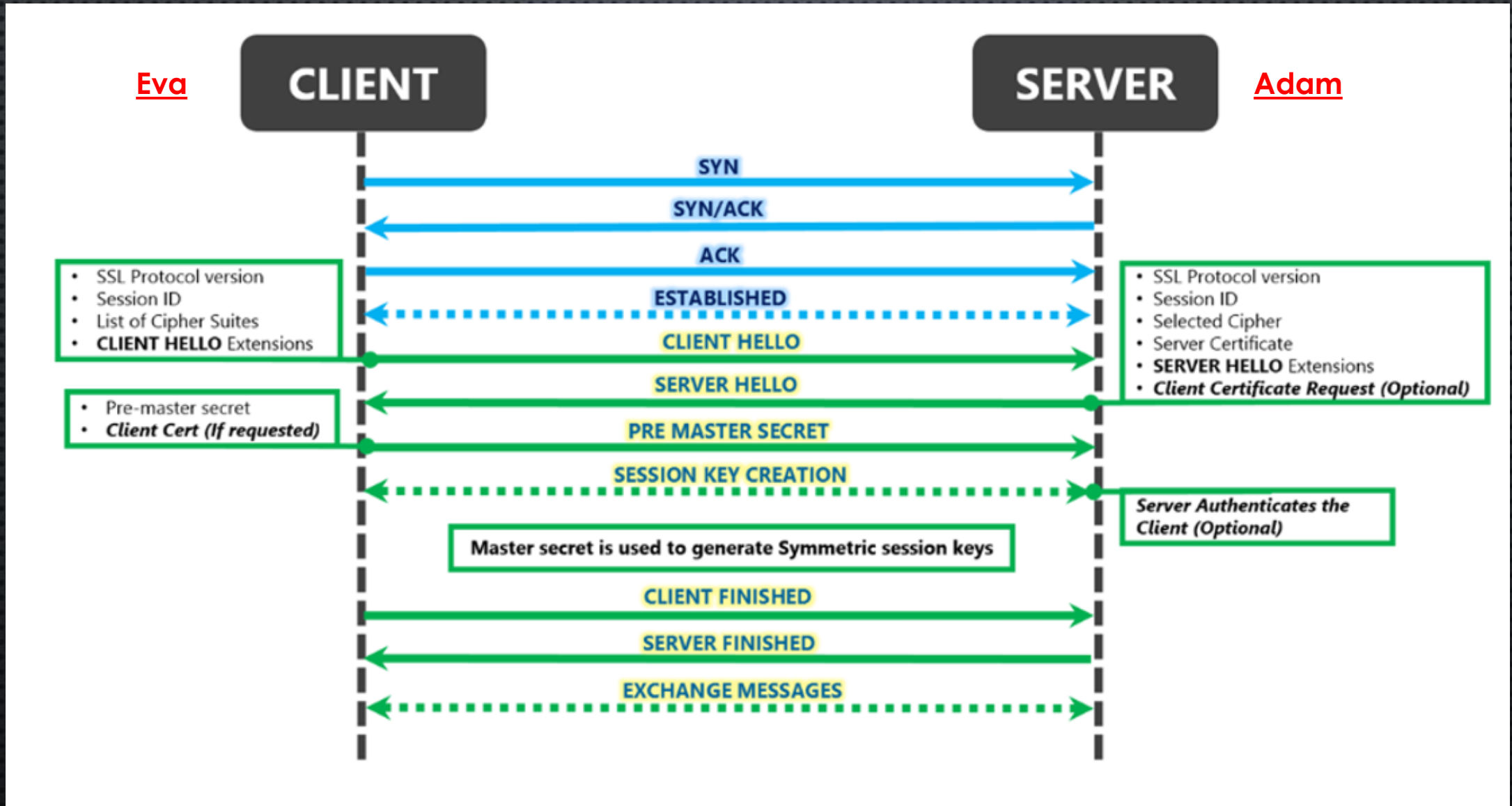


Certifikační a ověřovací proces

Kroky:

1. Adam požádá o vydání certifikátu od RA
2. RA schválí certifikační požadavek, pak RA požádá CA o vydání certifikátu pro Adama.
3. CA vydá certifikát pro Adam
4. CA aktualizuje centrální úložiště a certifikační revokační list (CRL) pro VA
5. Adam přidá certifikát do úložiště aplikace
6. Adamova Aplikace požádá o ověření platnosti certifikátu
7. VA kdykoliv ověří platnost certifikátu Adamovy Aplikace podle CRL

PŘÍKLAD TLS_RSA_WITH_AES_128_CBC_SHA256



ODKAZY

- RSA (cryptosystem) https://en.wikipedia.org/wiki/RSA_%28cryptosystem%29
- PKI https://en.wikipedia.org/wiki/Public_key_infrastructure
- Public-key cryptography https://en.wikipedia.org/wiki/Public-key_cryptography
- SHA-2 https://en.wikipedia.org/wiki/SHA-2
- CBC https://en.wikipedia.org/wiki/CBC-MAC
- AES https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

ODKAZY

- Microsoft Cryptographic Services https://msdn.microsoft.com/en-us/library/92f9ye3s(v=vs.110).aspx
- SSL Handshake and HTTPS Bindings on IIS http://blogs.msdn.com/b/kaushal/archive/2013/08/03/ssl-handshake-and-https-bindings-on-iis.aspx
- The Transport Layer Security (TLS) Protocol Version 1.2 http://tools.ietf.org/html/rfc5246
- Transmission Control Protocol http://tools.ietf.org/html/rfc793
- Internet Protocol http://tools.ietf.org/html/rfc791
- IP Authentication Header http://tools.ietf.org/html/rfc4302

ODKAZY

- Security/Server Side TLS https://wiki.mozilla.org/Security/Server_Side_TLS
- OpenSSL Ciphers https://www.openssl.org/docs/manmaster/apps/ciphers.html
- Black Hat - Hacking Windows Internals https://www.blackhat.com/presentations/bh-europe-05/BH_EU_05-Cerrudo/BH_EU_05_Cerrudo.pdf

KRYPTOSYSTÉMY

- OTÁZKY A ODPOVĚDI

KRYPTOSYSTÉMY

- DĚKUJI ZA POZORNOST