



LABKA KRYPTOSYSTÉMY

AUTOR: ADAM LICHNOVSKÝ

DATUM: 3.5.2017

OBSAH



- ÚVOD
- KRYPTOGRAFICKÉ SYSTÉMY
- OBECNÝ NÁVRH KRYPTOGRAFICKÉHO SYSTÉMU
- PUBLIC KEY INSTRUCTURE (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 GENEROVÁNÍ KLÍČŮ,
 - ALGORITMUS PRO ZAŠIFROVÁNÍ,
 - ALGORITMUS PRO ODŠIFROVÁNÍ.
- TERMÍN ŠIFRA (CIPHER, CYPHER) ČASTO OZNAČUJE PÁR ALGORITMŮ,
 - ALGORITMUS PRO ZAŠIFROVÁNÍ,
 - ALGORITMUS PRO ODŠIFROVÁNÍ.

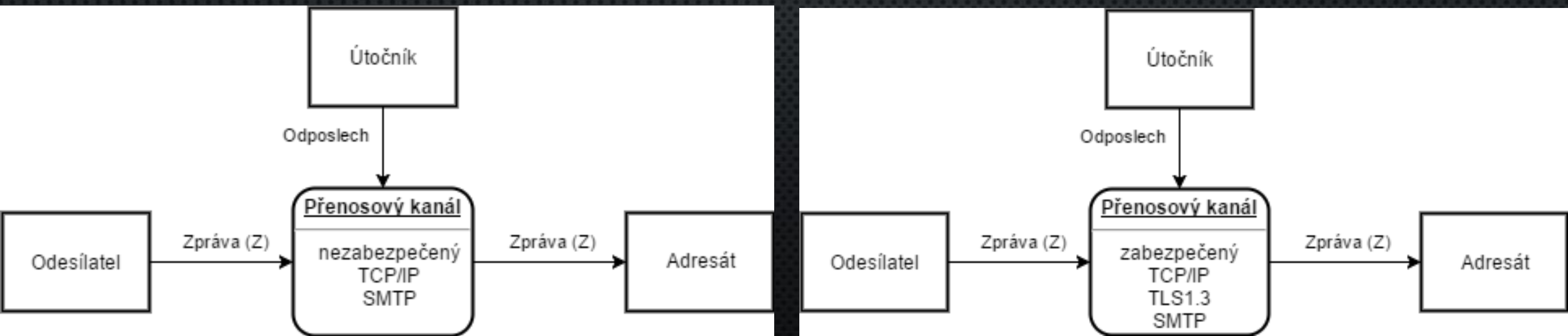
KRYPTOGRAFICKÉ SYSTÉMY

ŠIFRY

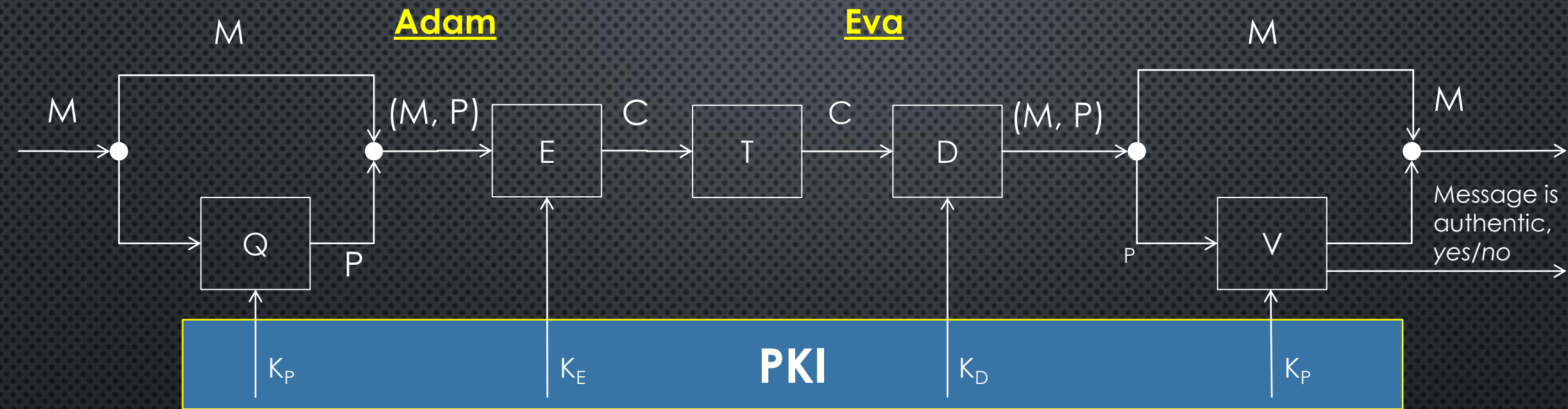
- ŠIFRA JE JAKÁKOLIV METODA ZAŠIFROVÁNÍ TEXTU PŘI ZACHOVÁNÍ ČITELNOSTI A VÝZNAMU. ČASTO SE ŠIFROU OZNAČUJE ZAŠIFROVANÝ TEXT ZPRÁVY, PŘESTO DÁLE BUDEME PREFEROVAT OZNAČENÍ KRYPTOGRAM.

KRYPTOGRAM

- ZAŠIFROVANÝ TEXT ZPRÁVY



OBEČNÝ 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

- K_P** – Veřejný klíč Adama
- K_E** – Šifrovací klíč (Privátní klíč Adama)
- K_D** – Dešifrovací klíč (Privátní klíč Evy)
- PKI** – Public Key Infrastructure

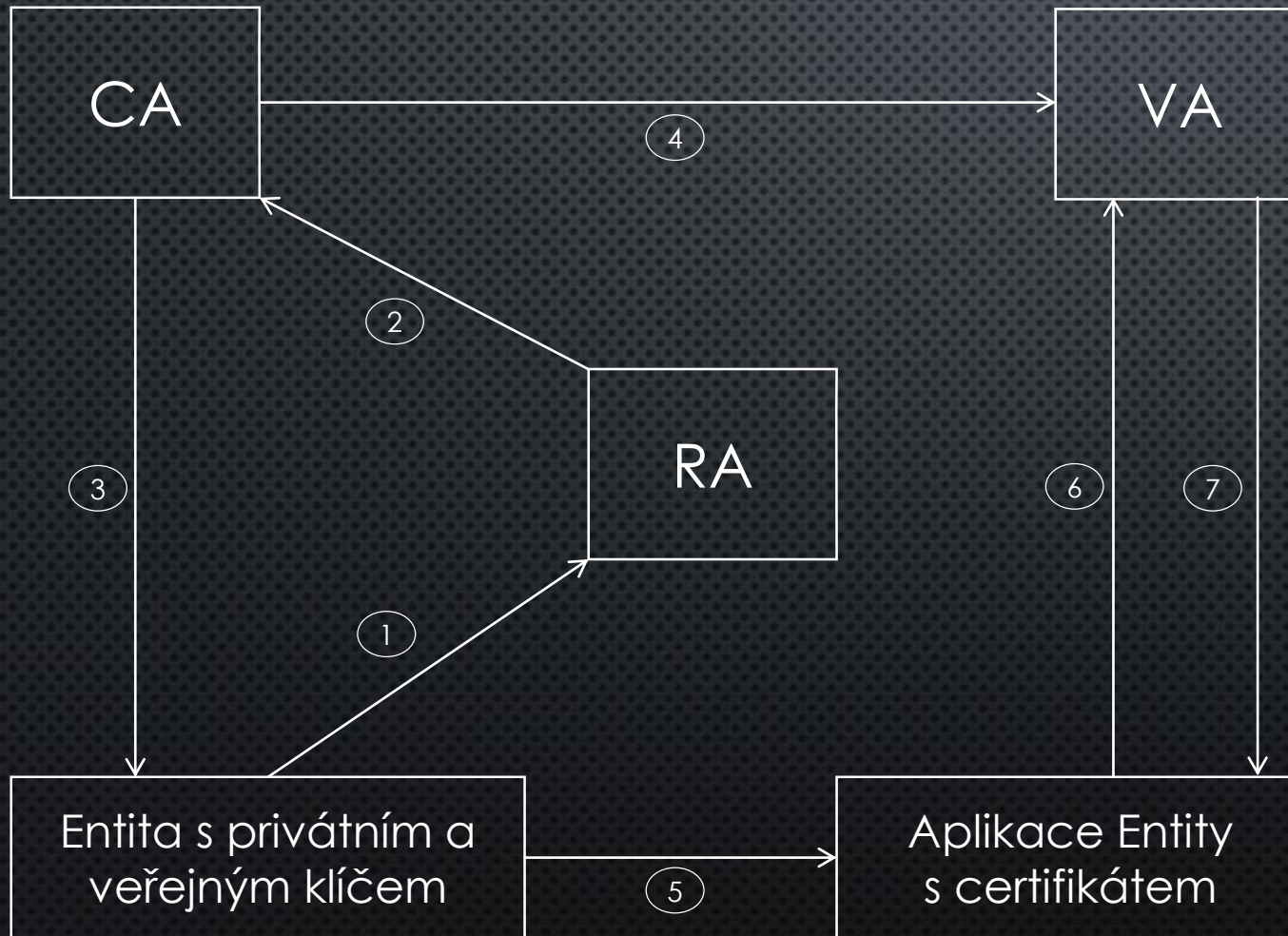
PUBLIC KEY INFRASTRUCTURE (PKI)

- 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 DIGITÁLNÍ 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 INTRASTRUCTURE (PKI)

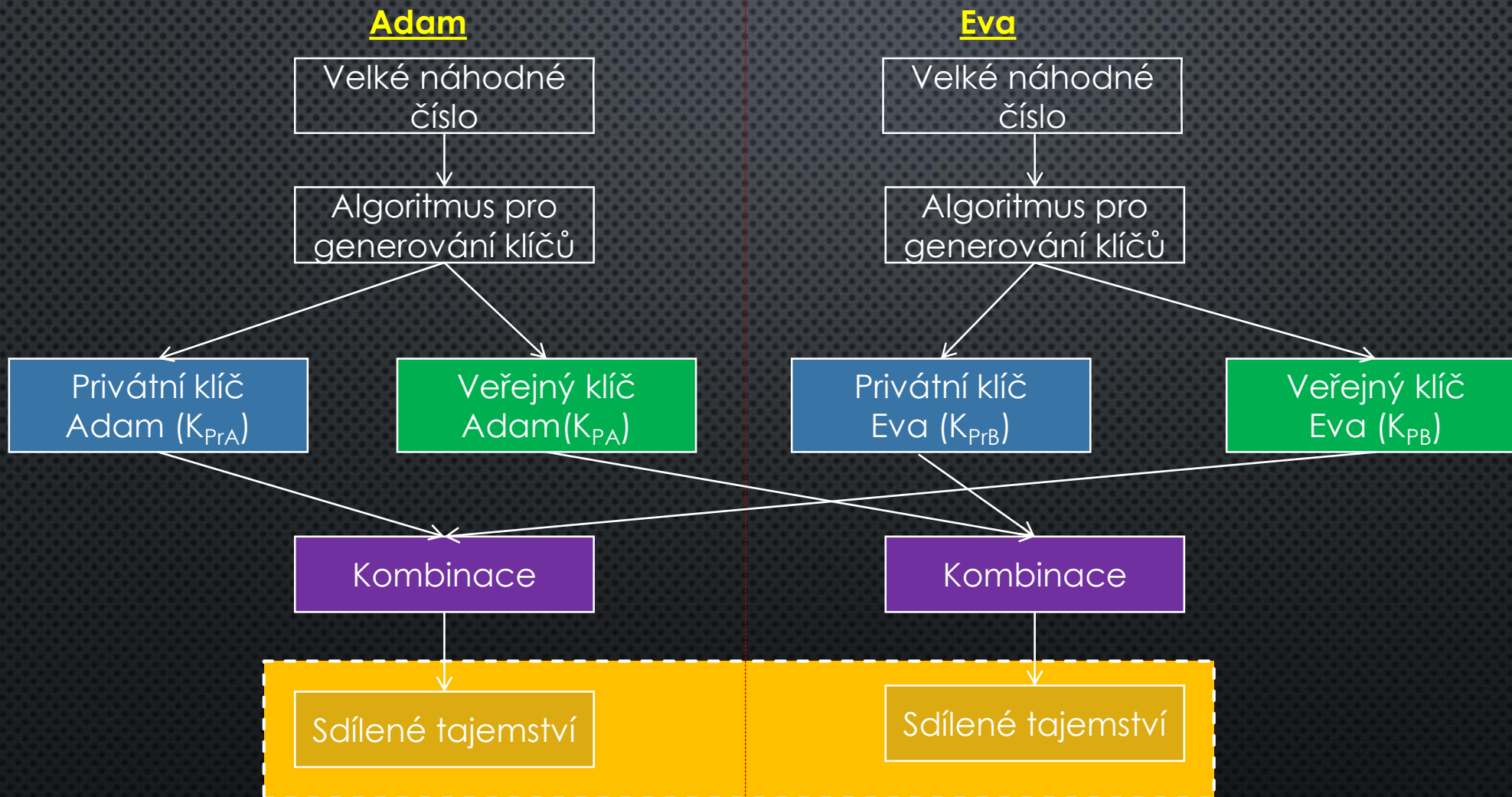


Certifikační a ověřovací proces

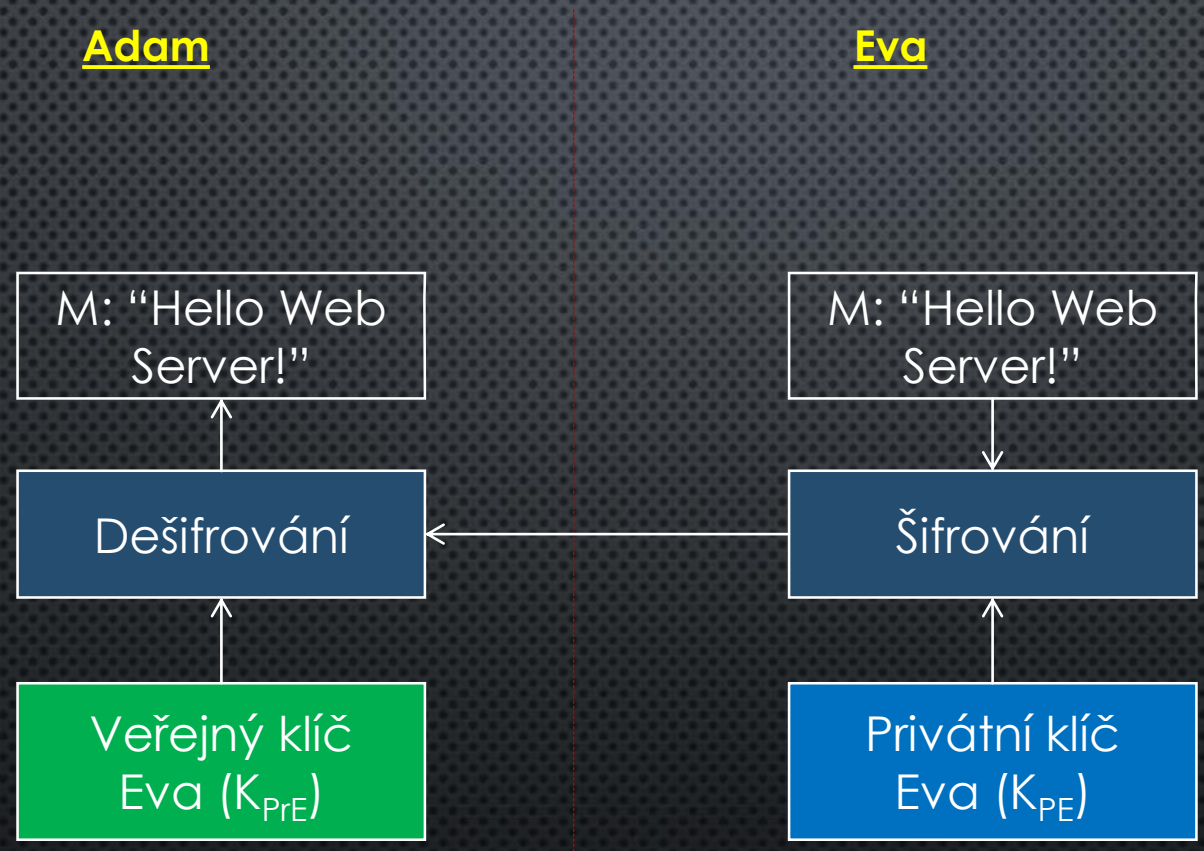
Kroky:

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. Entita přidá certifikát do úložiště aplikace
6. Aplikace Entity požádá o ověření platnosti certifikátu
7. VA kdykoliv ověří platnost certifikátu Aplikace Entity podle CRL

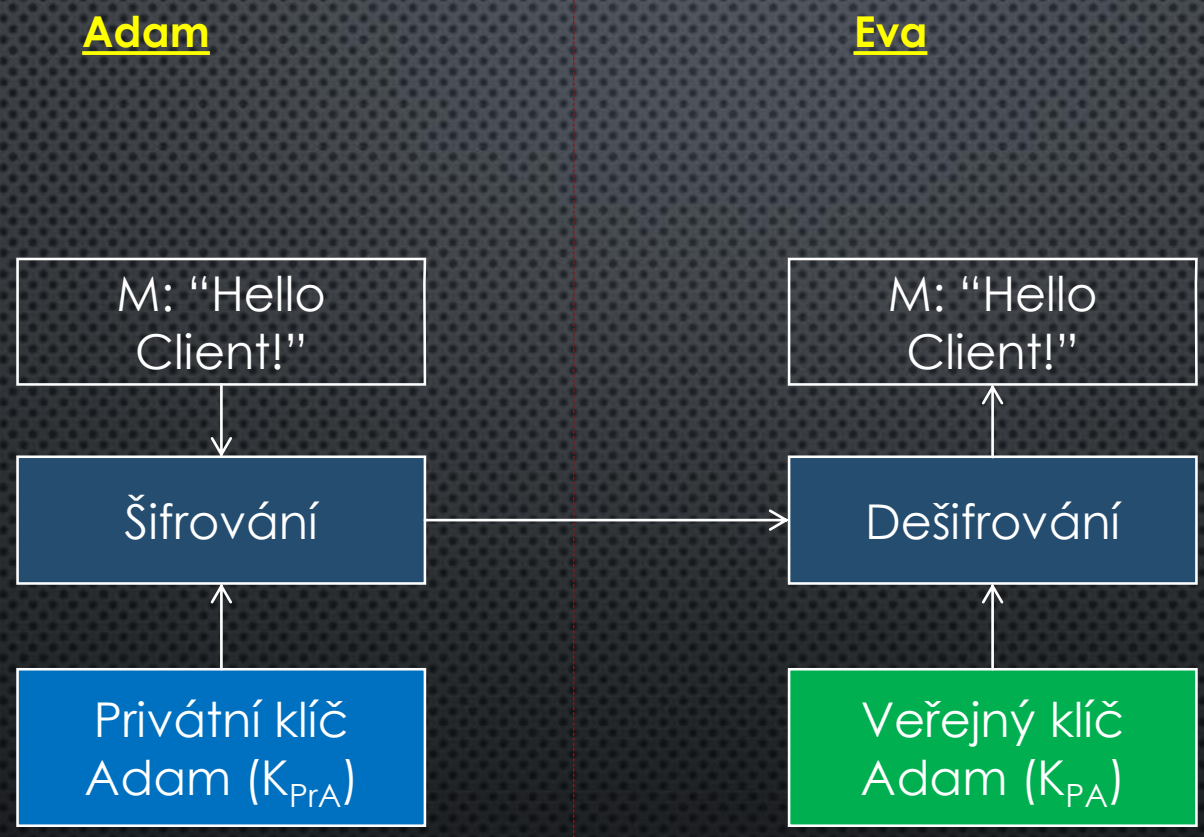
OBEČNÝ KRYPTOGRAFICKÝ SYSTÉM



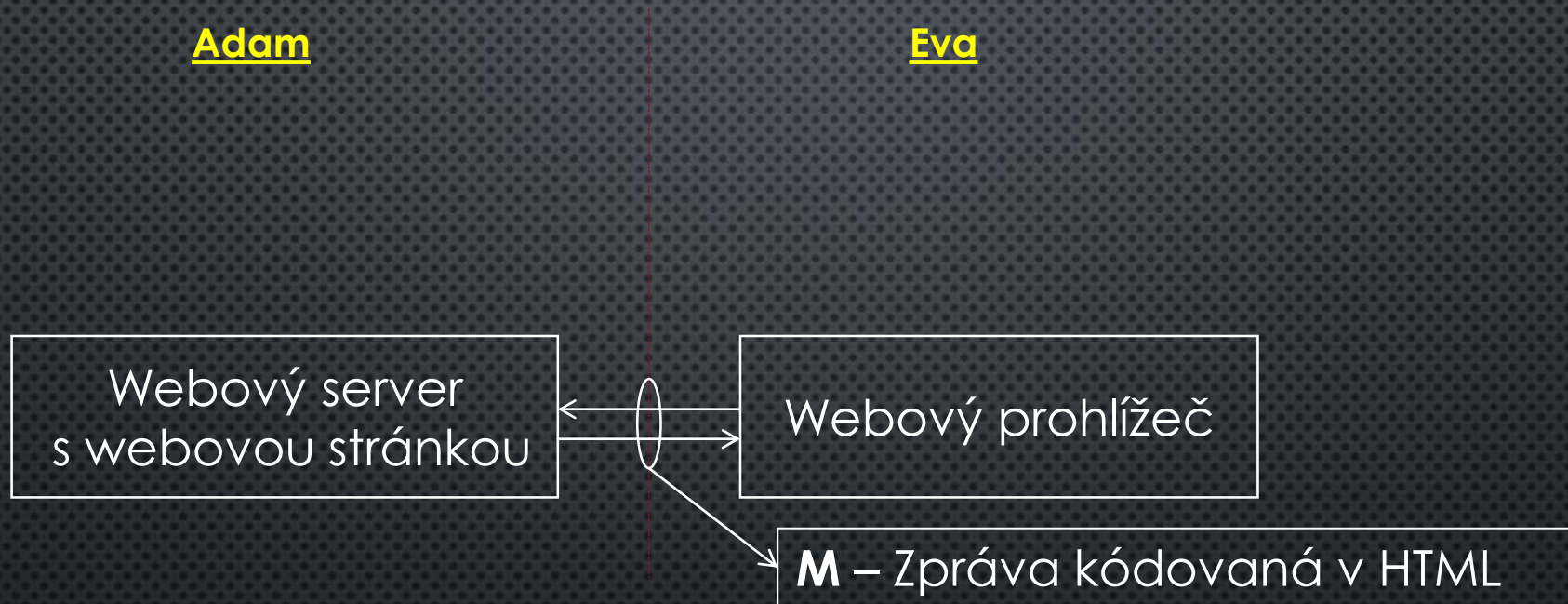
OBEČNÝ KRYPTOGRAFICKÝ SYSTÉM



OBECNÝ KRYPTOGRAFICKÝ SYSTÉM



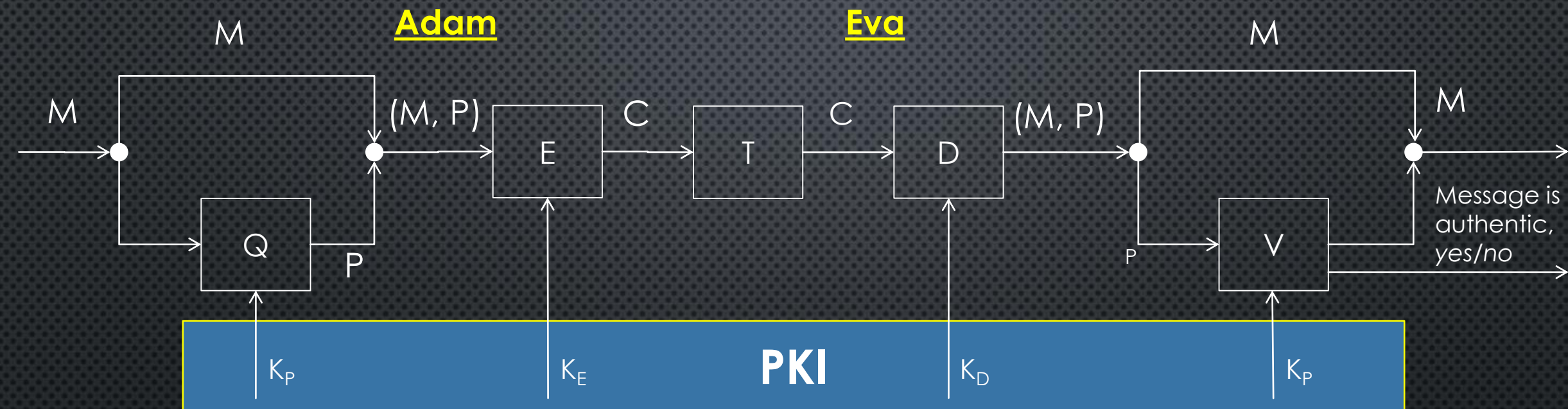
PŘÍKLAD TLS_RSA_WITH_AES_128_CBC_SHA256



Příklad:

Eva chce navštívit svou oblíbenou stránku svým oblíbeným webovým 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 – Veřejný klíč Adama

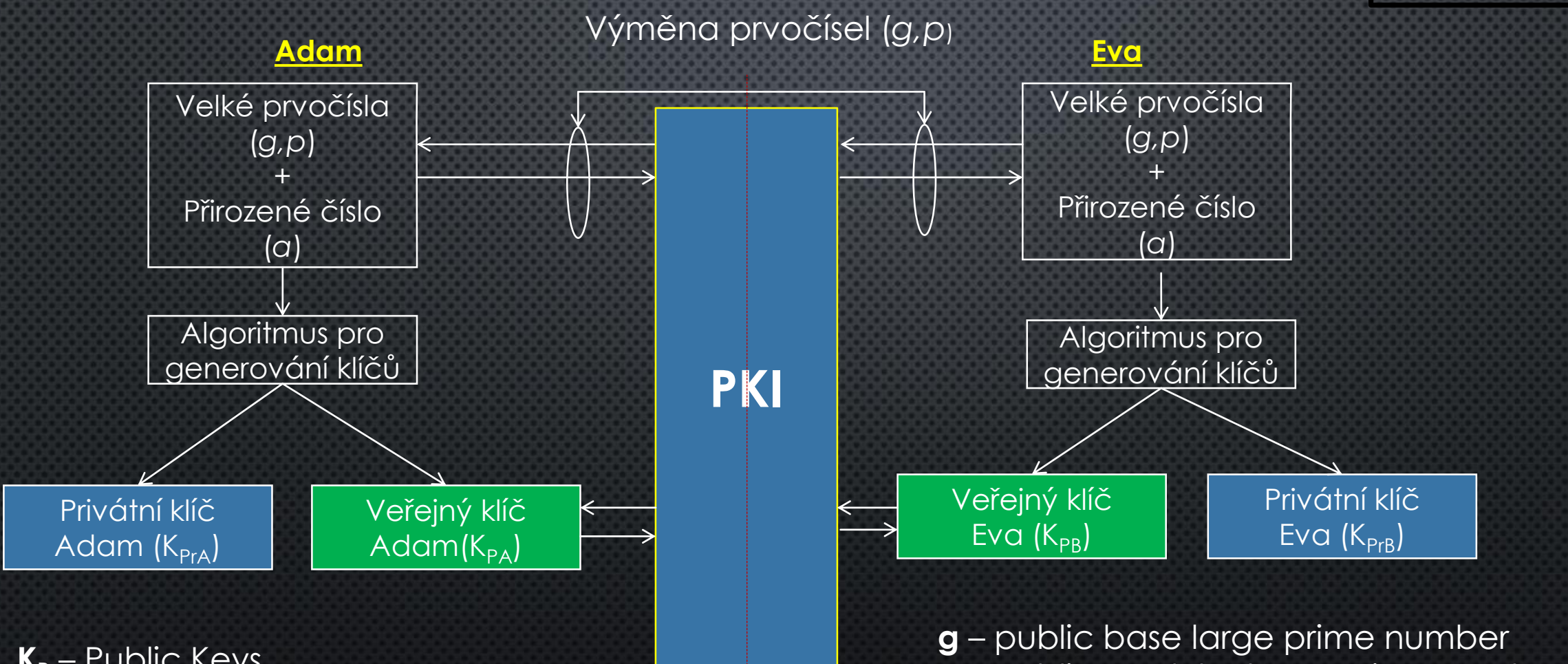
K_E – Šifrovací klíč (Privátní klíč Adama)

K_D – Dešifrovací klíč (Privátní klíč Evy)

PKI – Public Key Infrastructure

Message is authentic,
yes/no

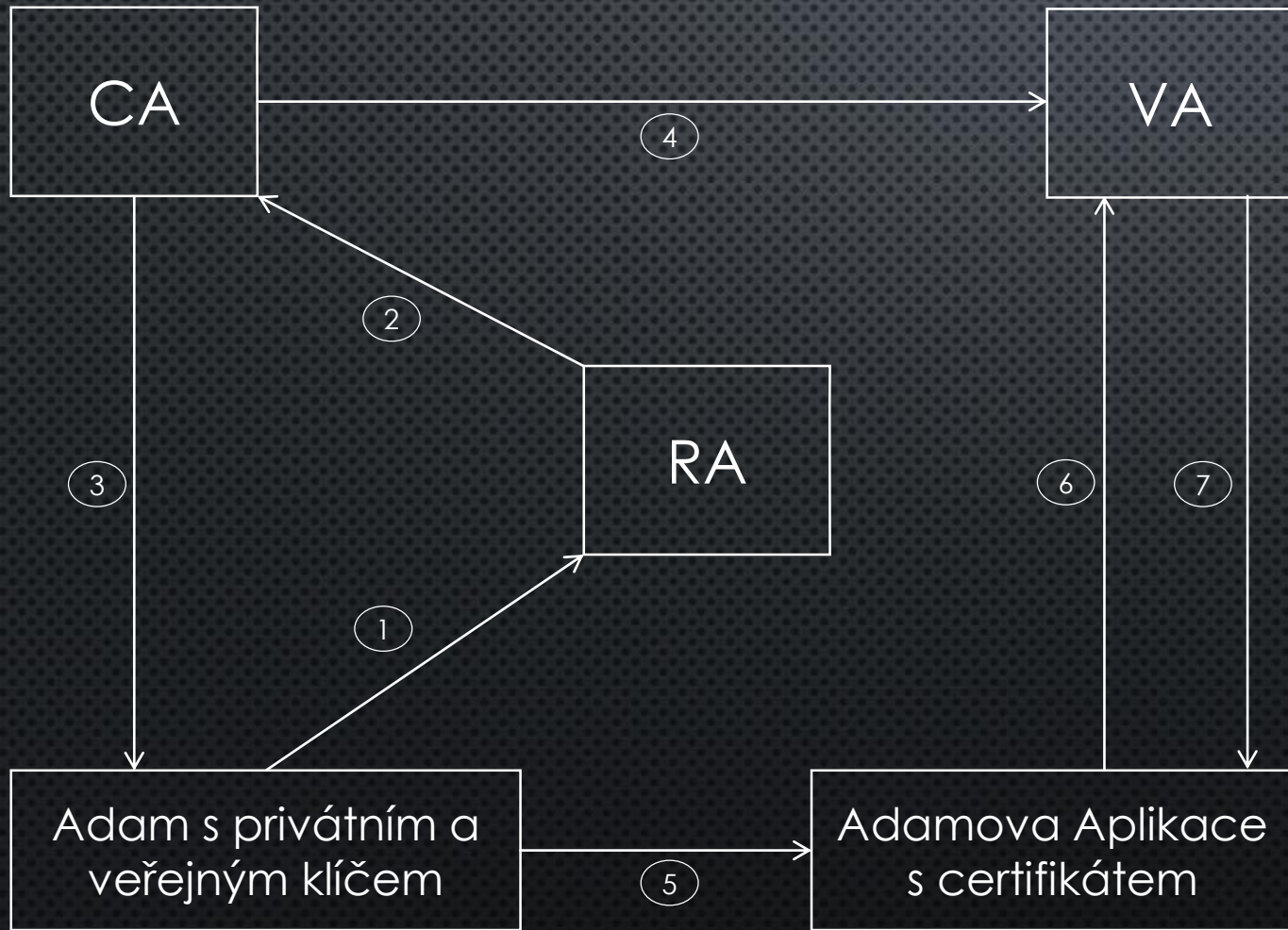
PŘÍKLAD TLS_RSA_WITH_AES_128_CBC_SHA256



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

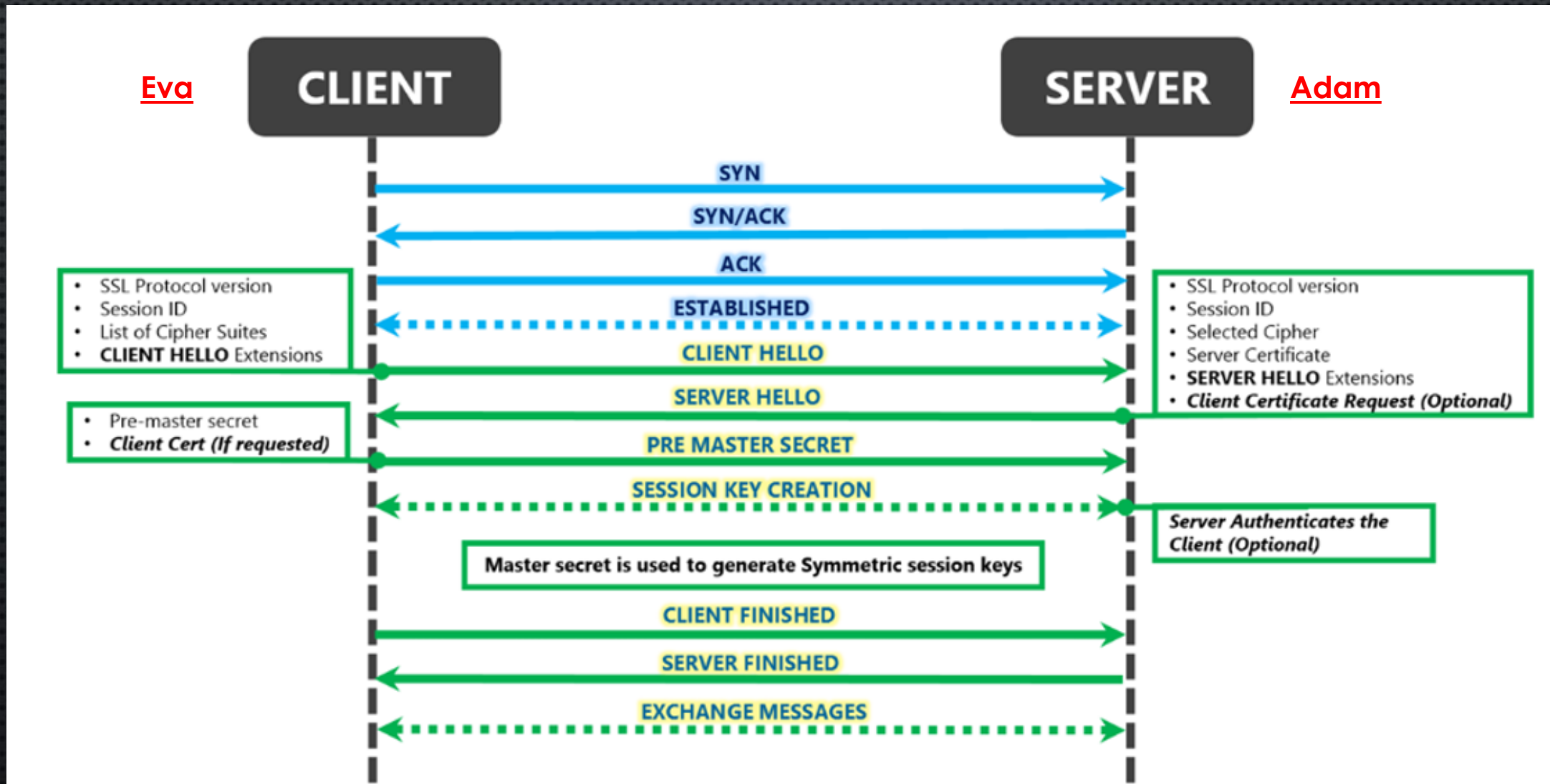


Certifikační a ověřovací proces

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](https://en.wikipedia.org/wiki/RSA_%28cryptosystem%29)
- PKI [HTTPS://EN.WIKIPEDIA.ORG/WIKI/PUBLIC_KEY_INFRASTRUCTURE](https://en.wikipedia.org/wiki/Public_key_infrastructure)
- PUBLIC-KEY CRYPTOGRAPHY [HTTPS://EN.WIKIPEDIA.ORG/WIKI/PUBLIC-KEY_CRYPTOGRAPHY](https://en.wikipedia.org/wiki/Public-key_cryptography)
- SHA-2 [HTTPS://EN.WIKIPEDIA.ORG/WIKI/SHA-2](https://en.wikipedia.org/wiki/SHA-2)
- CBC [HTTPS://EN.WIKIPEDIA.ORG/WIKI/CBC-MAC](https://en.wikipedia.org/wiki/CBC-MAC)
- AES [HTTPS://EN.WIKIPEDIA.ORG/WIKI/ADVANCED_ENCRYPTION_STANDARD](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard)

ODKAZY

- MICROSOFT CRYPTOGRAPHIC SERVICES [HTTPS://MSDN.MICROSOFT.COM/EN-US/LIBRARY/92F9YE3S\(V=VS.110\).ASPX](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](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](http://tools.ietf.org/html/rfc5246)
- TRANSMISSION CONTROL PROTOCOL [HTTP://TOOLS.IETF.ORG/HTML/RFC793](http://tools.ietf.org/html/rfc793)
- INTERNET PROTOCOL [HTTP://TOOLS.IETF.ORG/HTML/RFC791](http://tools.ietf.org/html/rfc791)
- IP AUTHENTICATION HEADER [HTTP://TOOLS.IETF.ORG/HTML/RFC4302](http://tools.ietf.org/html/rfc4302)

ODKAZY



- SECURITY/SERVER SIDE TLS [HTTPS://WIKI.MOZILLA.ORG/SECURITY/SERVER_SIDE_TLS](https://wiki.mozilla.org/Security/Server_Side_TLS)
- OPENSSL CIPHERS [HTTPS://WWW.OPENSLL.ORG/DOCS/MANMASTER/APPS/CIPHERS.HTML](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](https://www.blackhat.com/presentations/BH-EUROPE-05/BH_EU_05-CERRUDO/BH_EU_05_CERRUDO.PDF)

- OTÁZKY A ODPOVĚDI

KRYPTOSYSTÉMY



- DĚKUJI ZA POZORNOST