DOMAT
ČLEN ČEZ ESCO

Roadshow 2025

www.domat.cz

Program

- SCADA a co dál
- Nová řada IRC
- Kyberbezpečnost

SCADA exit

Důvody

- CRA a s ním spojená rizika
- Použité technologie a řešení (alarming)
- Priority vývoje

SCADA exit

CRA – v ČR Nařízení 2024/2847

Požadavky na kybernetickou bezpečnost

- Žádné známé zranitelnosti.
- Výchozí konfigurace zabezpečena. V případě custom řešení mít možnost návrat do původního stavu.
- Automatické bezpečnostní aktualizace, případně prostřednictvím oznamování dostupných aktualizací uživatelům.
- Zajištěná ochrana před neoprávněným přístupem vhodnými kontrolními mechanismy, mimo jiné na základě systémů správy ověřování, identity nebo přístupu, a podávají zprávy o možném neoprávněném přístupu.
- Při přenášení údajů využívat šifrování.
- Základní a klíčové funkce musí být dostupné i po incidentu
- Navrženy, vyvinuty a vyrobeny tak, aby:

- se omezily prostory k útoku, včetně vnějších rozhraní,

- se snížil dopad incidentu použitím vhodných mechanismů a technik zmírňujících zneužití.

- Zaznamenávají a kontrolují příslušnou interní činnost, včetně přístupu k údajům, službám nebo funkcím či jejich změn, s možností využít mechanismus výjimky pro uživatele.
- Poskytují uživatelům možnost bezpečně a snadno natrvalo odstranit všechny údaje a nastavení, a pokud mohou být tyto údaje přeneseny do jiných produktů nebo systémů, zajišťují, aby se tak stalo bezpečným způsobem.

SCADA exit

CRA – v ČR Nařízení 2024/2847

Část II Požadavky na řešení zranitelností

Výrobci produktů s digitálními prvky:

1) určí a zdokumentují zranitelnosti a komponenty obsažené v produktech s digitálními prvky, mj. na základě vypracování softwarového kusovníku (SBOM) v běžně používaném strojově čitelném formátu, který obsahuje přinejmenším nejdůležitější závislosti produktu,

2) v souvislosti s riziky, která pro produkty s digitálními prvky představují, neprodleně řeší a odstraňují zranitelnosti, mj. na základě poskytování bezpečnostních aktualizací; v případě, že je to technicky možné, jsou bezpečnostní aktualizace poskytovány odděleně od funkčních aktualizací,

3) provádějí účinné a pravidelné testy a pravidelný přezkum bezpečnosti produktu s digitálními prvky,

4) po zveřejnění bezpečnostní aktualizace poskytují a uveřejňují informace o opravených zranitelnostech, včetně popisu těchto zranitelností, informací umožňujících uživatelům zjistit dotčený produkt s digitálními prvky, dopadu zranitelností, jejich závažnosti a jasných a přístupných informací, které uživatelům pomáhají tyto zranitelnosti odstranit; v řádně odůvodněných případech, pokud se výrobci domnívají, že bezpečnostní rizika spojená se zveřejněním převažují nad bezpečnostními přínosy, mohou oddálit zveřejnění informací týkajících se opravy zranitelností až do doby, kdy budou mít uživatelé možnost příslušnou opravu použít,

5) zavádějí a prosazují politiku koordinovaného zveřejňování zranitelností,

6) přijímají opatření ke snadnějšímu sdílení informací o možných zranitelnostech svého produktu s digitálními prvky a o komponentách třetích stran obsažených v daném produktu, mimo jiné poskytnutím kontaktní adresy pro oznamování zranitelností zjištěných v produktu s digitálními prvky,

7) stanovují mechanismy pro bezpečnou distribuci aktualizací produktů s digitálními prvky s cílem zajistit, že zranitelnosti budou včas opraveny nebo zmírněny, a že se tak bude u bezpečnostních aktualizací dít automaticky, je-li to možné,

8) zajišťují, aby v případě, že jsou k dispozici bezpečnostní aktualizace pro řešení zjištěných bezpečnostních problémů, byly neprodleně, a pokud neexistuje jiná dohoda mezi výrobcem a podnikatelským uživatelem s ohledem na produkt s digitálními prvky zhotovený na zakázku, bezplatně šířeny spolu s poradními zprávami, které uživatelům poskytují relevantní informace, včetně informací o možných opatřeních, jež je třeba přijmout.

SCADA exit

Termíny

30.4.2025	oznámení o ukončení produktu (po tomto datu nenabízet)
1.7.2025	vyřazení z ceníku (po tomto datu neprodávat)
30.6.2027	ukončení vydávání aktualizací a relicencování (maximálně do tohoto data by měla být poskytována záruka)
31.12.2027	ukončení technické podpory

SCADA exit

Alternativy

Geovap – **Reliance** (SSCP)

ICONICS – **Genesis** (BACnet)

Microsys – **Promotic** (BACnet)

Energocentrum Plus s.r.o. - **Mervis SCADA** - hostované řešení (SSCP, SoftPLC Link pro starší systémy)

Alfa Mikrosystémy – **ProCop** (BACnet, SoftPLC Link)

Pokojové ovladače a regulátory

DUC

room control unit
standalone or with *DFCR*
68 × 60 mm backlit display
24 V AC / DC
communicative

RS485 Modbus

CO_2

** in black or white housing*

DUC219

heating / cooling controller
68 × 60 mm backlit display
2 DI, 2 DO SSR
24 V AC / DC
communicative

RS485 Modbus

CO_2

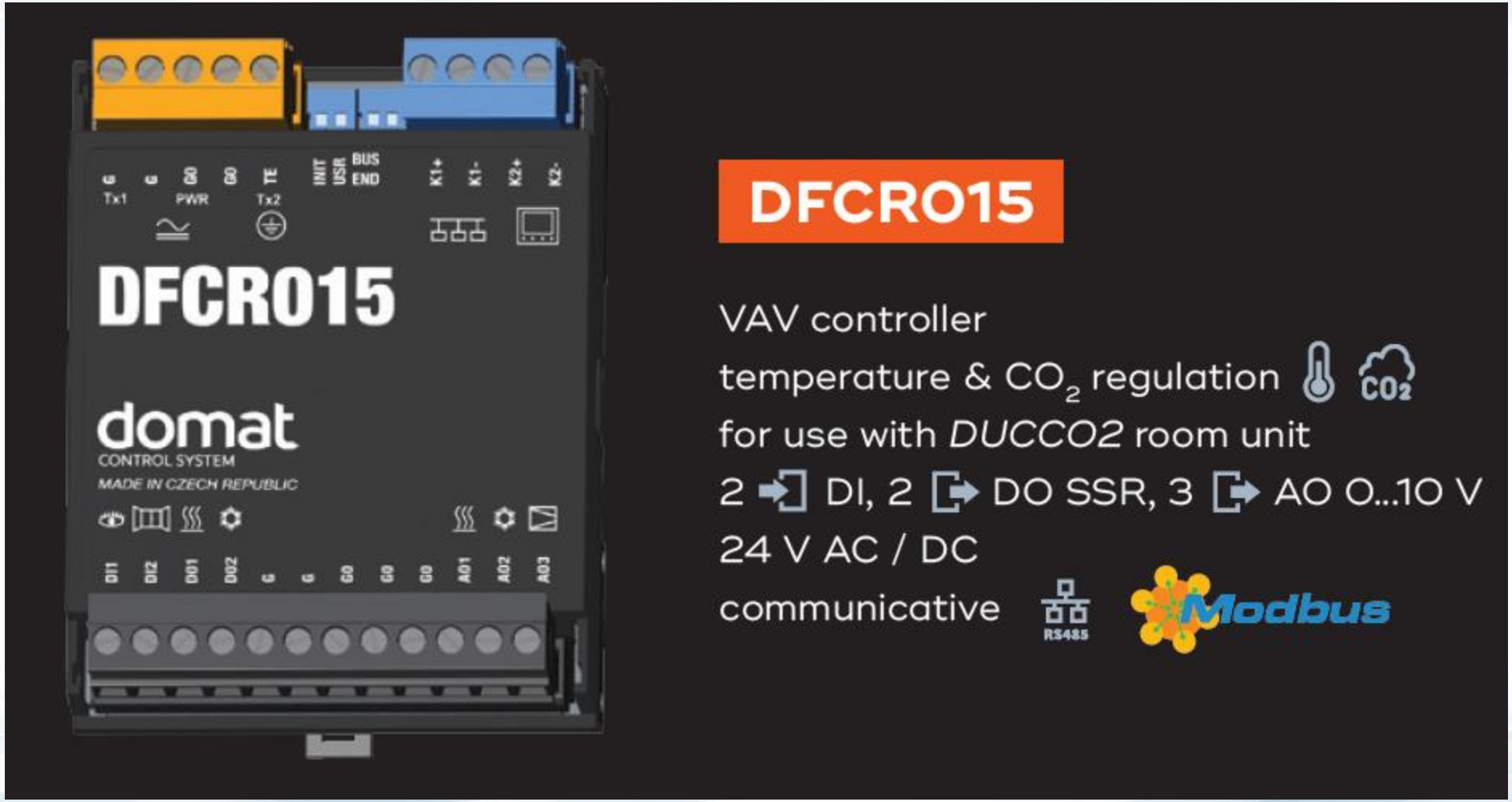
** in black or white housing*

Pokojové ovladače a regulátory

Pokojové ovladače a regulátory

Pokojové ovladače a regulátory

Pokojové ovladače a regulátory



Pokojové ovladače a regulátory

Přehled

EPC103 + ST1W	EPC102, regulátor topení do veřejných prostor
DFCR010, 011	regulátor FC + T + CH, 3x relé + 2x triak, 24 nebo 230 V
DFCR013	regulátor FC + T + CH, 3x 0...10 V + 2x triak
DFCR015	regulátor CO2 + T + CH, 3x 0...10 V + 2x triak
DUC	ovladač k DFCR10, 11, 13, PLC
DUCCO2	ovladač k DFCR15
DUC200/209/219	regulátor T + CH, měř. rH / +CO2 / + CO2 +PIR
BM230 / 300	zadní modul, 2 DI, 2 triak / + AI Pt1000

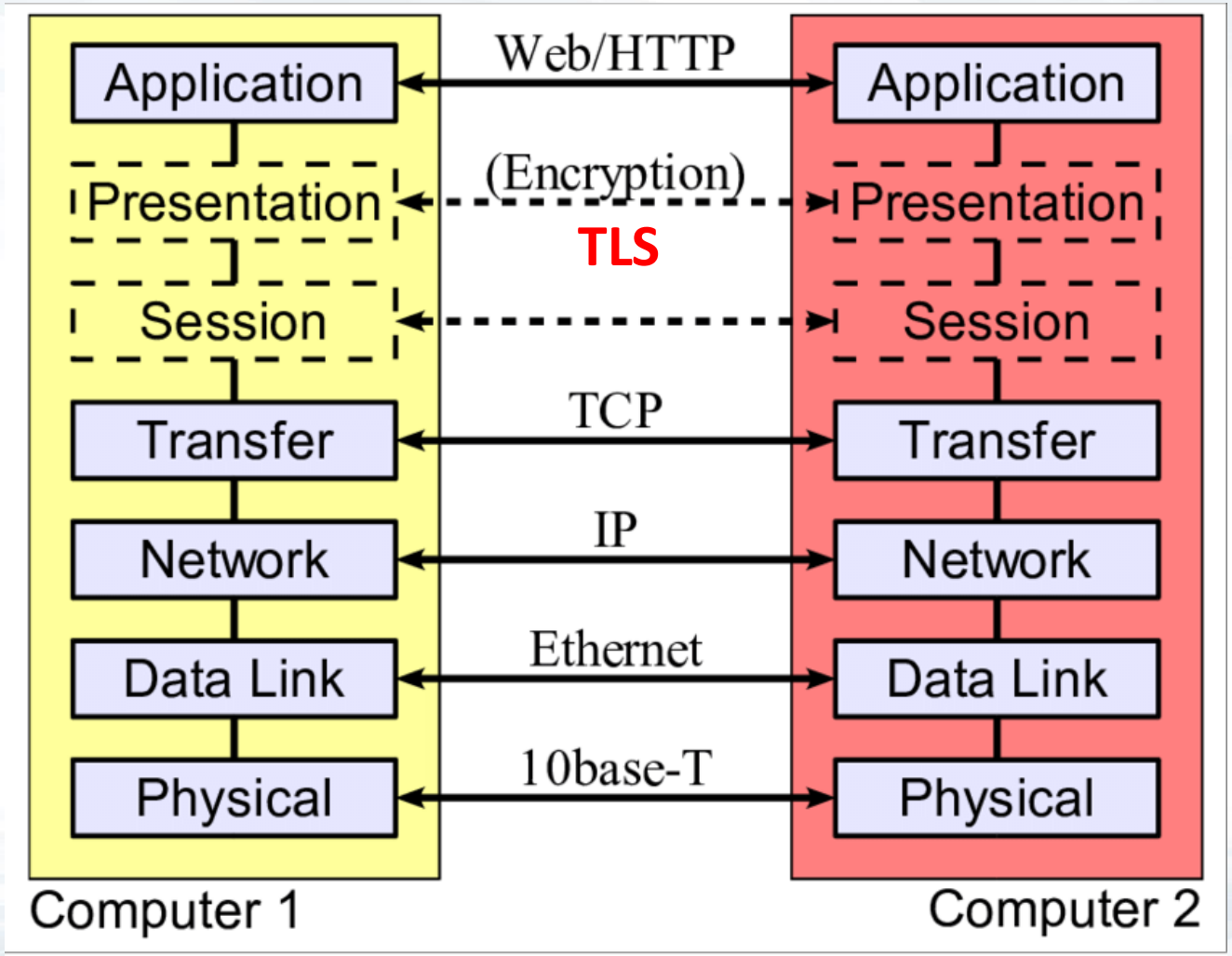
TLS

- Základní principy – TLS, veřejný a privátní klíč
- Výměna klíčů
- Ověřování: Certifikáty, řetězení certifikátů
- Nahrávání do PLC
- Komunikační scénáře a jejich vlastnosti

TLS

- Transport Layer Security

ve vrstvě
Session / Presentation



Bez TLS

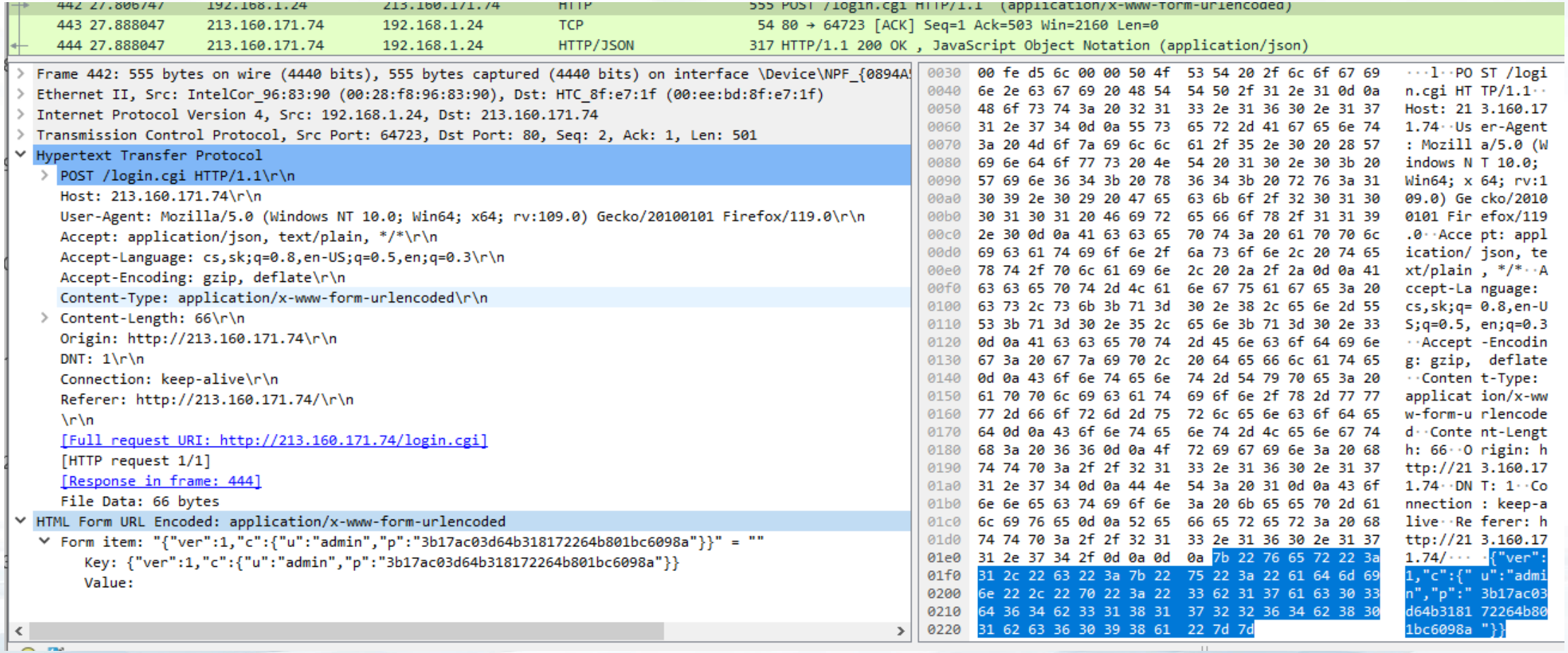
V programu Wireshark:

Ethernet

IP

TCP

data



TLS

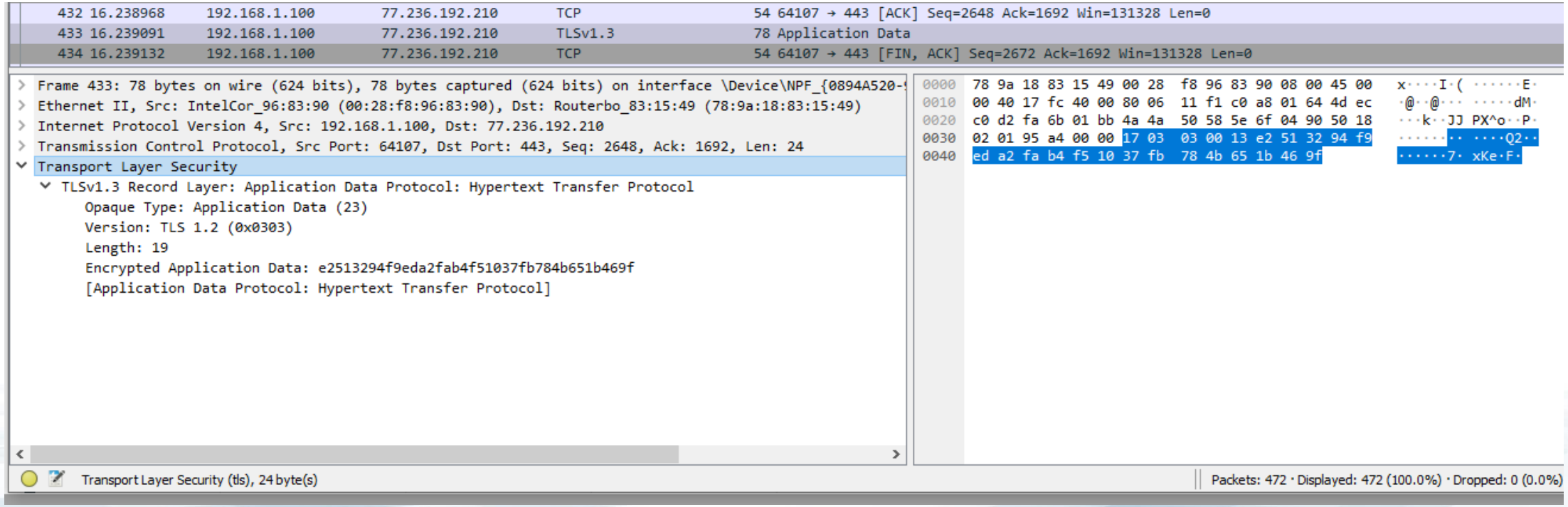
V programu Wireshark:

Ethernet

IP

TCP

TLS



Základní principy

Řešíme dva problémy:

- **šifrování** - znečitelnění komunikace pro cizí subjekty
- **ověřování -** prokázání (serveru), že strana je ta, za kterou se vydává

Symetrické šifrování

- rychlé
- problém: identický klíč nutno bezpečně nasdílet

Asymetrické šifrování

- pomalejší – výpočetně náročnější
- ale možnost bezpečné výměny (sdíleného tajného) klíče veřejným kanálem !

Základní principy

Postup:

- navázání spojení klient -> server
- dohodnutí pravidel a standardů
- pomocí asymetrického šifrování výměna symetrického klíče
- případně ověření serveru vůči klientovi
- použití symetrického klíče pro přenos dat
  (= méně výpočetně náročné, než asymetrické šifrování)
- ukončení spojení

Základní principy

Z aplikačního hlediska potřebujeme zajistit podmínky pro úvodní asymetrické šifrování:

- pár „veřejný klíč + privátní klíč“

- **veřejný klíč**: server dává k dispozici (libovolné) protistraně – slouží pro zašifrování zpráv
- **privátní klíč**: uložen „nečitelně“ na serveru (ideálně v chipu - TPM),
  slouží pro dešifrování zpráv, nesmí být zveřejněn

Navázání spojení a získání symetrického klíče

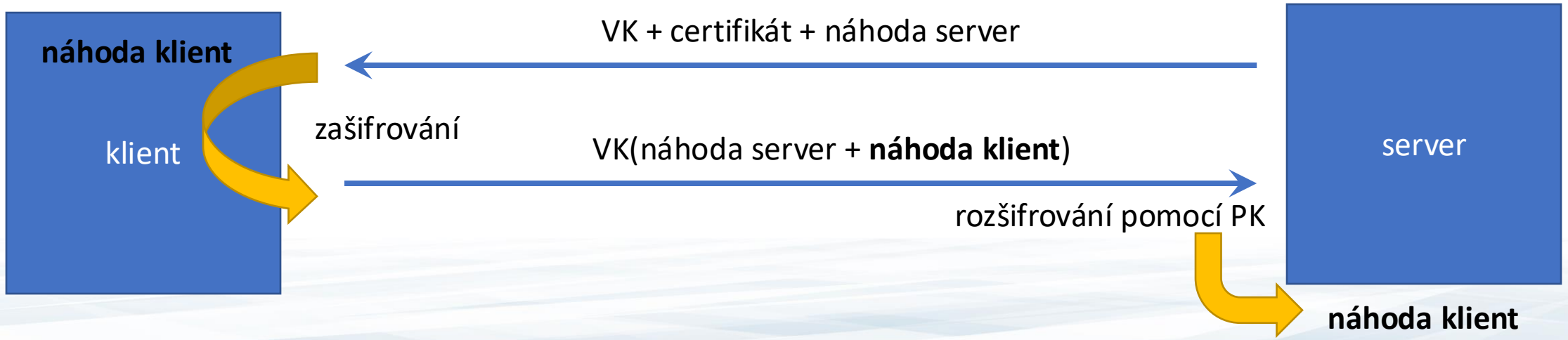
Postup:

- klient naváže spojení se serverem, požádá o zabezpečené spojení,
- **server pošle veřejný klíč** a certifikát, dále pošle náhodně generovaný klíč,
- klient zkombinuje tento náhodný klíč se svým náhodně generovaným klíčem,
- **klient použije veřejný klíč k zašifrování** celé kombinace,
- následně zašifrovanou kombinaci pošle na server,
- **server rozšifruje pomocí svého privátního klíče** (který nikdo jiný nezná),
- tím získá mj. klientský náhodný klíč,
- tento **klientský náhodný klíč tedy znají obě strany a přitom nemohl být cestou nikde přečten nikým cizím**,
- s jeho pomocí se dále realizuje (symetricky) šifrovaná výměna informací.

Navázání spojení a získání symetrického klíče

Postup:

- **server pošle veřejný klíč** a **certifikát**, dále pošle náhodně generovaný klíč
- **klient použije veřejný klíč k zašifrování** kombinace náhodných klíčů,
- **server rozšifruje pomocí svého privátního klíče** (který nikdo jiný nezná)



Certifikát

K čemu je dobrý?

Důvěryhodná infomace o tom, co je server zač.

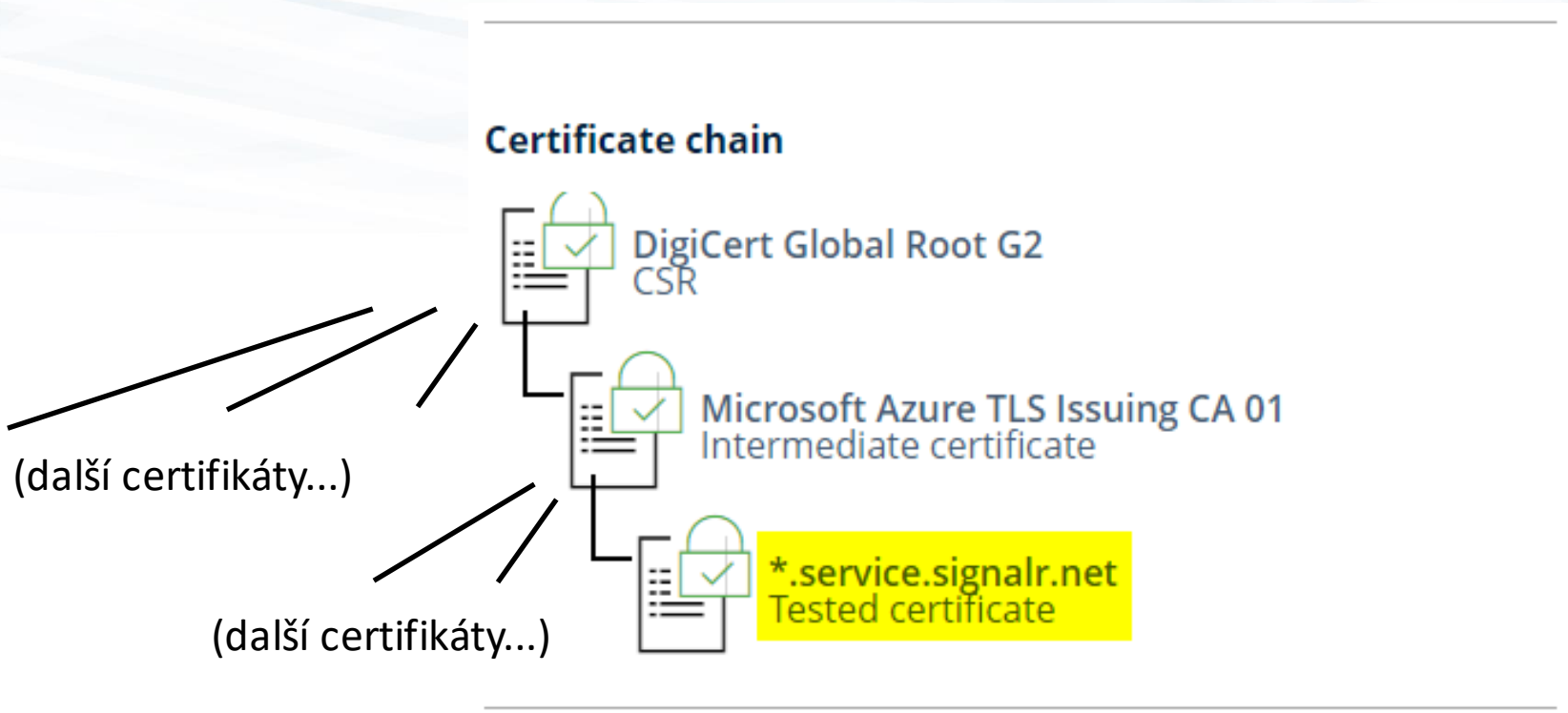
Klient ho ověřuje proti (stejnému) certifikátu, který má (nebo proti *řetězci důvěry*).

- **self-signed** – certifikát podepsaný sám sebou („vizitka“), klient ho
  - buď akceptuje bez dalších pochyb, což je případ spojení **bez validace certifikátu**,
  - nebo porovná s tímtéž certifikátem, který má nahraný v adresáři s důvěryhodnými certifikáty (**user_ca**).
- **podepsaný autoritou**, a to
  - **vlastní** – („průkazka“) - ověření proti autoritě, na kterou je navázán. Doménový certifikát nebo jeho kořenová autorita musí být nahrán u klienta v **user_ca**. Pokud je certifikát nahrán u klienta, musel ho tam nahrát autor celého bezpečnostního konceptu a klient mu tedy důvěřuje.
  - **veřejnou** – ("občanka") - ověření proti nějaké veřejné autoritě, což je nejvyšší stupeň důvěryhodnosti. Certifikát příslušné autority musí být opět nahrán u klienta v adresáři s certifikáty standardních autorit **user_ca**. Operační systém Windows obvykle základní (kořenové) certifikáty obsahuje, jinak je lze naimportovat.

  Autority lze řetězit.

Certifikát – řetězec důvěry

Příklad:



Stačí, aby klient měl u sebe certifikát veřejné autority (zde DigiCert) a je schopen ověřit, že certifikát MS Azure je v pořádku - a tedy i .service.signalr.net, který se na něj odvolává, je OK.

Certifikát

Jak certifikát vzniká?

Generuje ho *certifikační autorita*.

V žádosti je mj.

- veřejný klíč,
- informace o držiteli certifikátu, jako jméno, firma, e-mail, země atd.,
- informace o typu a délce klíče, např. RSA 2048.

Doba platnosti (max. 2 roky, self-signed až 30 let)

Součástí certifikátu je i veřejný klíč (aby protistrana mohla zasílat šifrované zprávy).

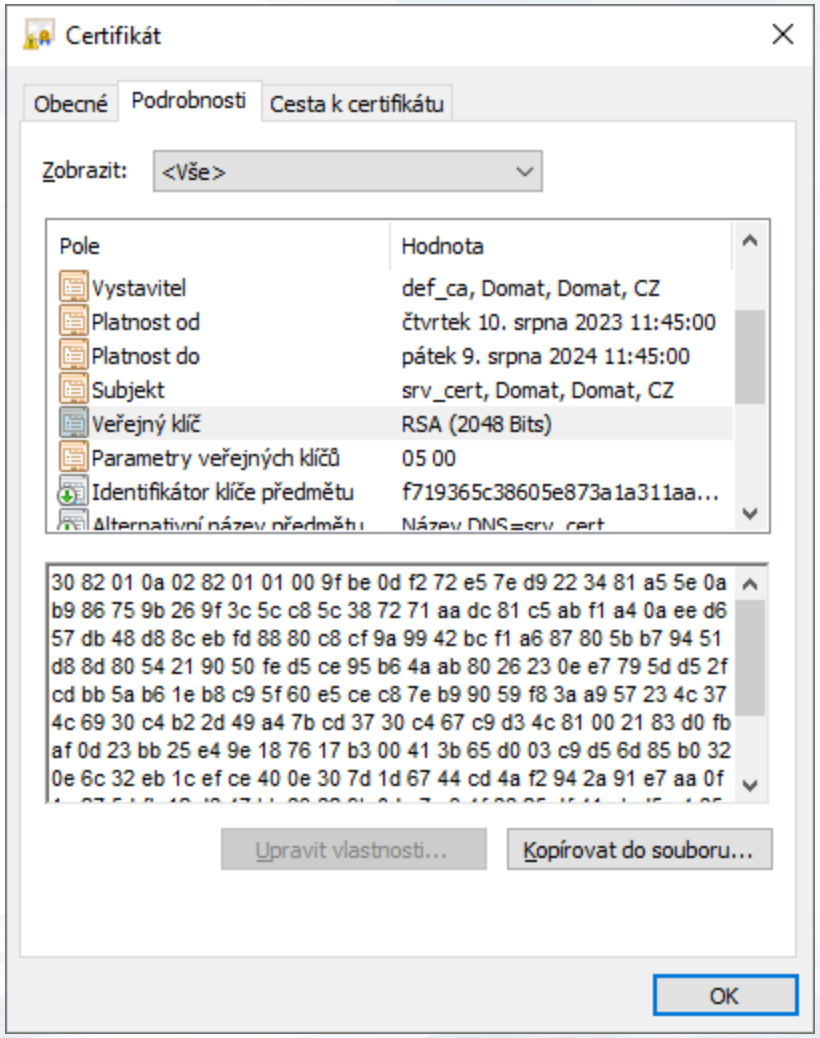
Předání privátních klíčů: osobní převzetí, heslo jiným kanálem atd.

Certifikát

Jak vypadá?

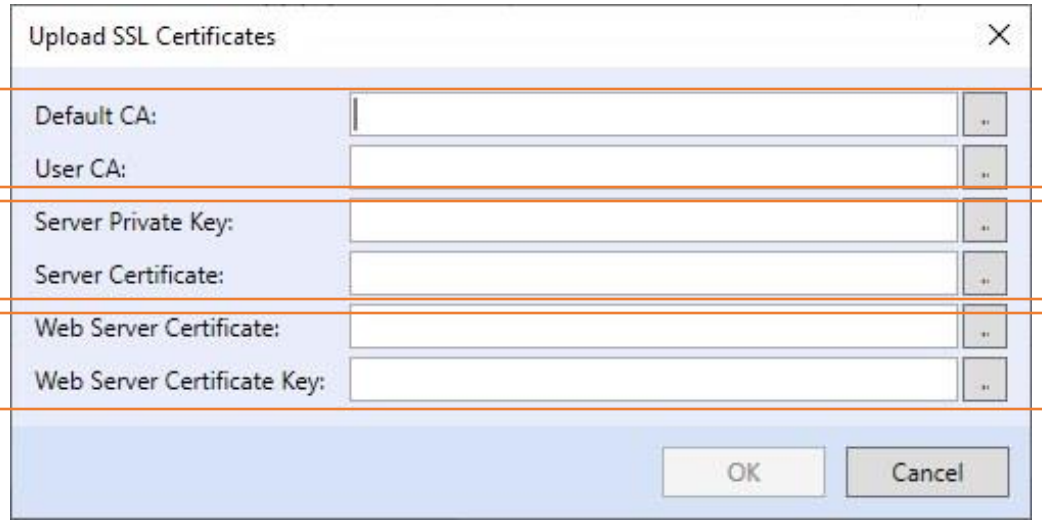
domat_server_cert.crt

```
-----BEGIN CERTIFICATE-----
MIIDoTCCAomgAwIBAgIIRX65y+Pes+MwDQYJKoZIhvcNAQELBQAwPjELMAkGA1UE
BhMCQ1oxDjAMBgNVBAoTBURvbWF0MQ4wDAYDVQQLEwVEb21hdDEPMA0GA1UEAwwG
ZGVmX2NhMB4XDTIzMDgxMDEwNDUwMFoXDTI0MDgwOTEwNDUwMFowQDELMAkGA1UE
BhMCQ1oxDjAMBgNVBAoTBURvbWF0MQ4wDAYDVQQLEwVEb21hdDERMA8GA1UEAwwI
c3J2X2N1cnQwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCfvg3ycuV+
2SI0gaVeCrmGdZsmnzxcyFw4cnGq3IHFq/GkCu7WV9tI2Izr/YiAyM+amUK88aaH
gFu31FHYjYBUIZBQ/tXOlbZKq4AmIw7neV3VL827WrYeuMlfYOXOyH65kFn4OqlX
I0w3TGkwxLItSaR7zTcwxGfJ00yBACGD0PuvDSO7JeSeGHYXswBBO2XQA8nVbYWw
Mg5sMusc785ADjB9HWdEzUrylCqR56oPGidd+xLWR7tjYpsN58NPaCXfQavVpGVe
sq5rB8aXjevW6Q7qDqv8VsqiciVqsyPXcdYmSCP7LU64f0YKRpeBGCWEYqCkwSmz
lbDerOrSWNaLAgMBAAGjgaAwgZ0wDAYDVR0TAQH/BAIwADAdBgNVHQ4EFgQU9xk2
XDhgXoc6GjEaobxg3JJQgpIwDgYDVR0PAQH/BAQDAgPoMBYGA1UdJQEB/wQMMAoG
CCsGAQUFBwMBMBMGA1UdEQQMMAqCCHNydl9jZXJ0MBEGCWCGSAGG+EIBAQQEAwIG
QDAeBglghkgBhvhCAQ0EERYPeGNhIGNlcnRpZmljYXRlMA0GCSqGSIb3DQEBCwUA
A4IBAQCmnIPdqW4ccoaeFff3buyv3DcIMG4ipyRxW6Egk9KCCgtC8rk0VCNljuuA
64wDlOJE5HG9bSgumq69EKOFYmGT5d6t6S79A6gvlHbICAGE4YSP3pausKOrtIoH
ALe8ISz8khzwwWLVITBjCRlzRWCDO/QHR8rTCAX4U4sRImtSlbI5LqFlgScX7jWd
pYHdeM0bBlbrIgkLI/nwElMOidUHJAajKFfSNXI40p7xElssFhJxGhBjPrOig7/s
ysKNj5/IJO8Wdm6azAI9MhWknP9DZ3jtr3wsS2qsMoHXOo6s9qfWVIVbRvhdUwO6
8iG7cnakGuBRvzCnbvEl/RxYE5bS
-----END CERTIFICATE-----
```



Nahrávání do PLC

PLC – Operace s PLC – Nahrání certifikátů



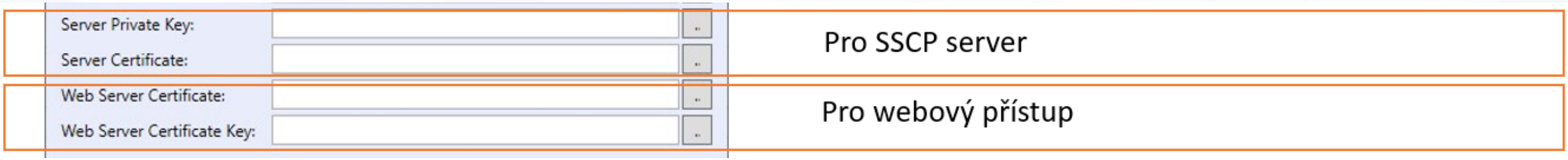
Pro Proxy server a Merbon DB (PLC je klientem)

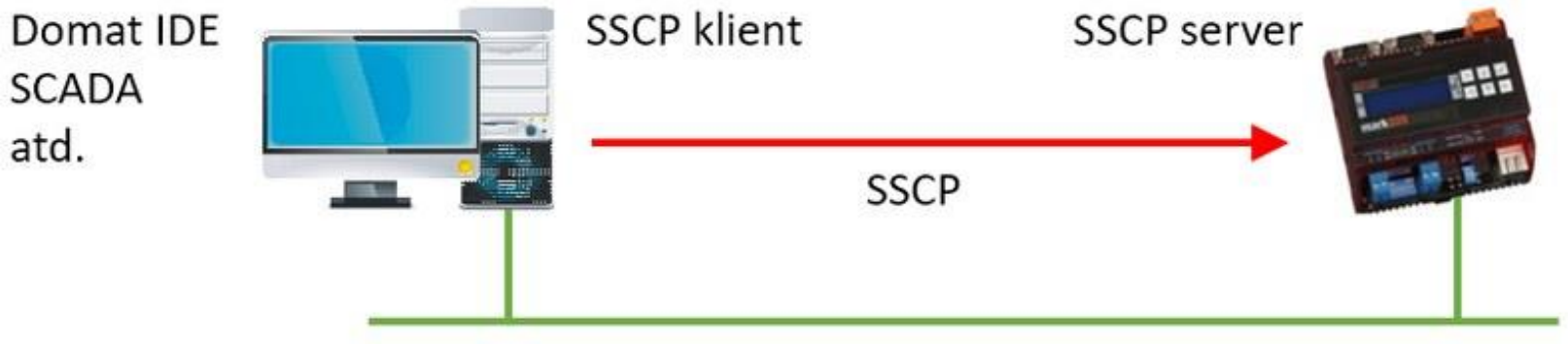
Pro SSCP server: certifikát + privátní klíč

Pro webový přístup: certifikát + privátní klíč

Nahrávání do PLC

PLC v roli klienta a **serveru** – rozlišovat!

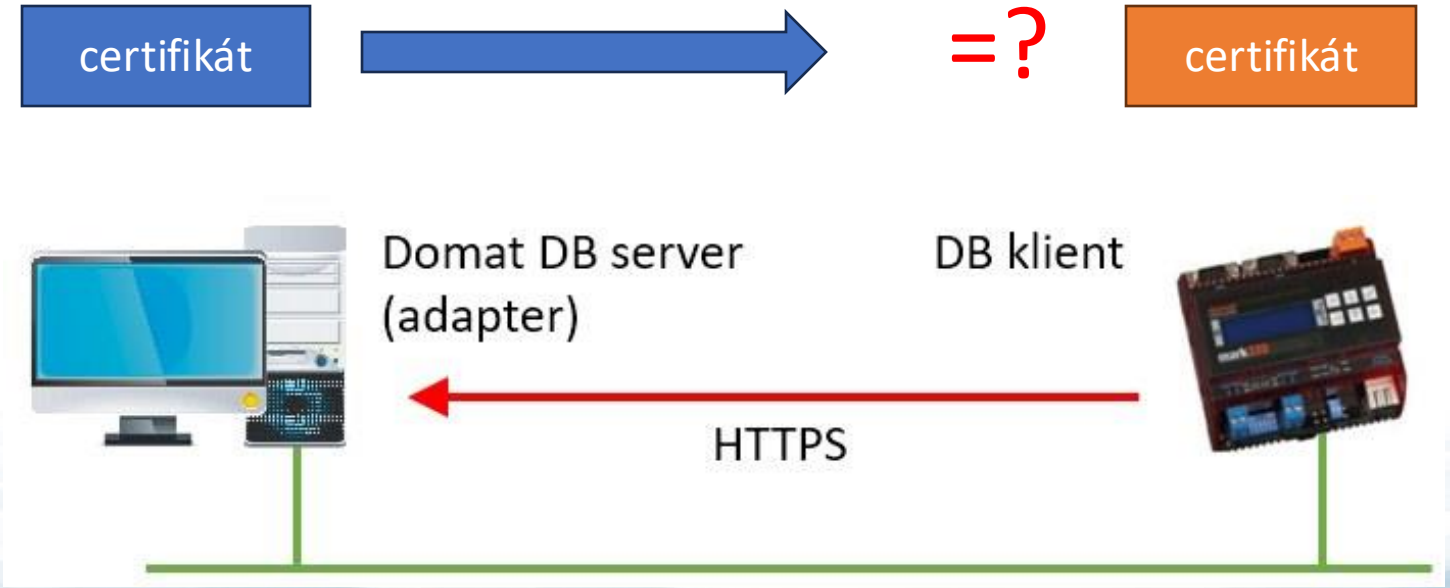




Nahrávání do PLC

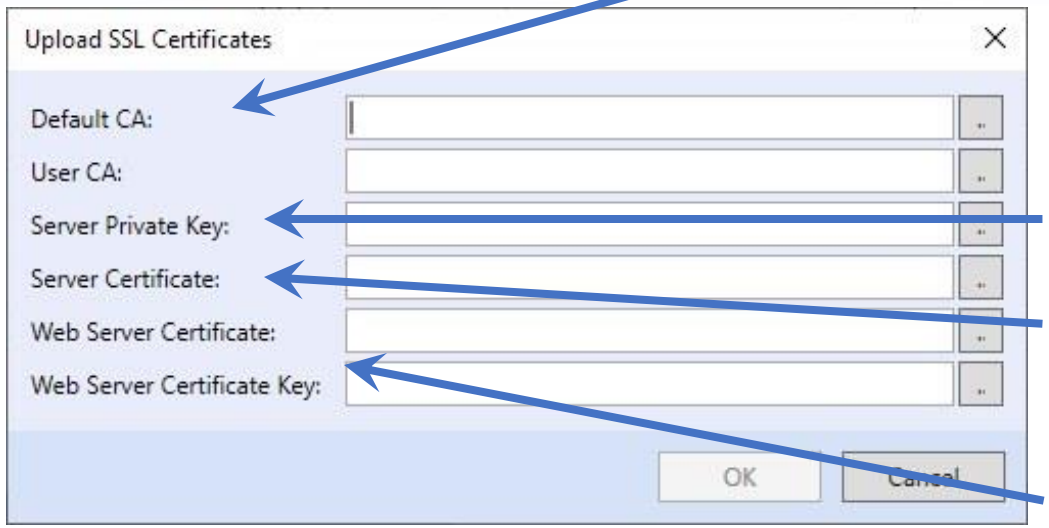
PLC v roli **klienta** a serveru – rozlišovat!

Pro Proxy server a Merbon DB (PLC je klientem)



Nahrávání do PLC

Jaké certifikáty a klíče jsou nahrány z výroby?



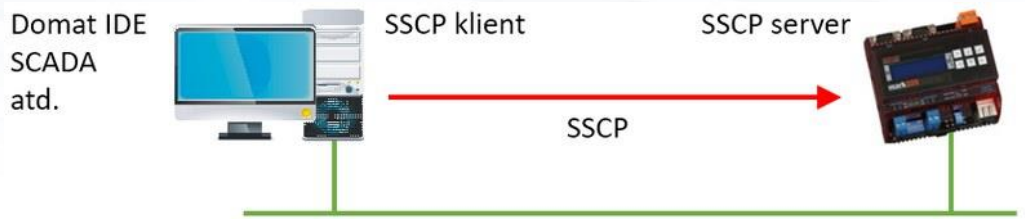
- **Výchozí CA** - z výroby je nahrán certifikát certifikační autority Domat. Je vyžadován pro spojení na Proxy server a databáze v rámci hostovaných služeb Domat, pokud je zaškrtnuta možnost Validace certifikátu.
- **Uživatelská CA** - z výroby nenahrán, sem je možné volitelně nahrát certifikát autority, používané uživatelem.
- **Privátní klíč serveru**, požadovaný pro bezpečné **SSCP spojení** (z IDE nebo jiných PLC). Privátní klíč je nahrán ve výrobě.
- **Serverový certifikát**, požadovaný pro bezpečné **SSCP spojení** (z IDE nebo jiných PLC). Ve výrobě se nahrává certifikát serveru podepsaný certifikační autoritou Domat.
- **Web server certificate** a **Web server certificate key** jsou požadované pro bezpečný **přístup na web (https://).** Certifikát a klíč pro produkční provoz musí poskytnout **správce domény, na níž je PLC web server provozován** (např. plc.firma.cz). Výchozí jsou pro doménu **plc.domat.cz**, tedy slouží především pro testování spojení.

Komunikační scénáře

- Klient (IDE, Visual, SCADA,...) se připojuje pomocí zabezpečeného SSCP na PLC jako na **server**.
- Webový prohlížeč se připojuje pomocí *https://* na PLC jako na **server**.
- PLC se připojuje jako **klient** k databázi (DB), chce uložit data.
- PLC se připojuje jako **klient** k mail serveru přes SMTPS, chce odeslat mail.
- PLC se připojuje jako **klient** na Merbon Proxy server.
- PLC se připojuje jako **klient** pomocí SSCP na jiné PLC (SSCP channel).

Komunikační scénáře

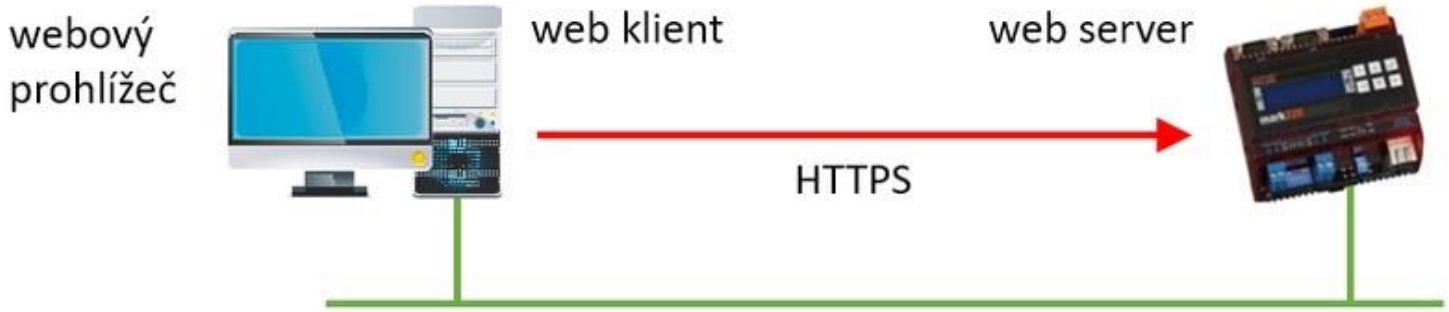
Klient (IDE, SCADA, ...) se připojuje pomocí SSCP na PLC



Bez zabezpečení - Běžná konfigurace, spojení SSCP na cílový port 12346. V IDE v Parametrech připojení není vybráno Povolení SSL, v konfiguraci PLC nemusí být SSL server povolen.
Zabezpečené spojení TLS bez ověřování - V IDE Povolení SSL, cílový port 12347.
V PLC musí být nahrán privátní klíč (srv_key) a certifikát s veřejným klíčem (srv_cert). Řeší se pouze znečitelnění komunikace pro cizí, ne ověřování identity stran.
Se serverovým certifikátem ve výchozím stavu - Součástí továrního nastavení je rovněž výchozí serverový certifikát. PLC má v souboru *def_ca* self-signed certifikát, který **vydala certifikační autorita Domat**, také self-signed (tedy neověřená proti veřejné autoritě), a protože tyto certifikáty jsou nahrány ve všech PLC, pro jejich vzájemné ověření jim to stačí i bez přístupu na Internet. Na PC s klientem (IDE, SCADA) nutno importovat certifikát také.
Se serverovým certifikátem, ověřování proti autoritě - Nutno vybavit klienta certifikátem vůči **autoritě na Internetu** (pak musí mít klient přístup na Internet), nebo certifikátem, který má PLC nahraný v user_ca - toto si zařídí uživatel, který buduje vlastní systém důvěry.

Komunikační scénáře

Webový prohlížeč se připojuje pomocí https:// na PLC



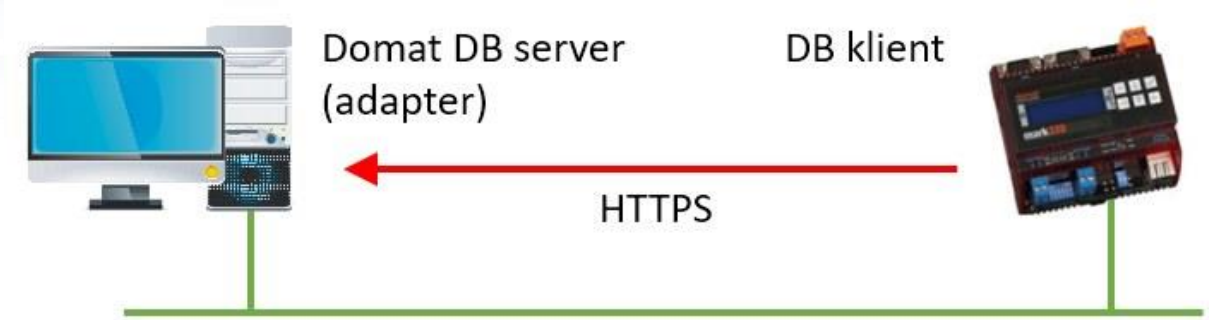
Bez zabezpečení - Spojení přes protokol *http://* (TCP port 80). Některé prohlížeče již umožňují přístup jen v místní síti, ne přes Internet; nutno odsouhlasit, že uživatel přistupuje na nezabezpečený web.

Zabezpečené spojení bez ověření domény - Spojení přes protokol *https://* (TCP port 443). Data jsou nečitelná pro cizí stranu, ale klient nemůže ověřit pravost domény, na které web server běží. Lze použít výchozí TLS certifikáty nahrané z výroby.

Zabezpečené spojení s ověřením domény - Spojení přes protokol *https://* (TCP port 443), navíc verifikace pomocí doménového certifikátu. Pro ně je nutné do PLC nahrát oba soubory "Web Server..." - certifikát a klíč. Web server certifikát musí být vystaven pro doménu, na které pak bude web server PLC pro klienta viditelný, tedy např. **plc.firma.cz**. Při tvorbě certifikátu se toto zadává v "common name". Certifikát zařizuje správce domény.

Komunikační scénáře

PLC se připojuje k databázi (DB), chce uložit data

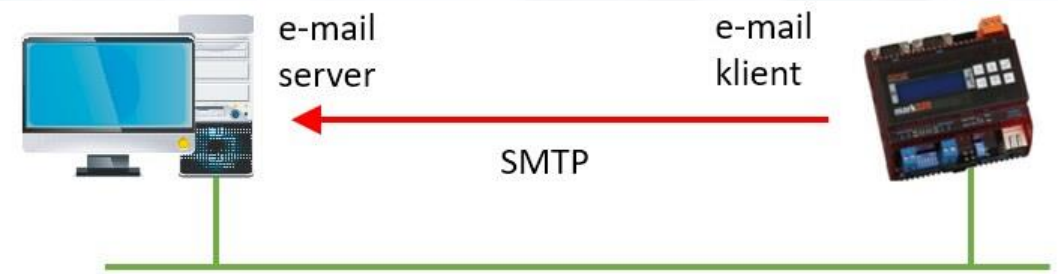


Nezabezpečené spojení: Standardní *http://* připojení k Domat DB adaptéru, adaptér ani PLC není nutno z hlediska bezpečnosti nijak konfigurovat.
Zabezpečené spojení bez validace domény: Zabezpečené spojení, v PLC stačí zadat URL ve tvaru *https://*. Do PLC není nutné nahrávat žádné certifikáty, klíče atd.
Zabezpečené spojení s validací domény: V PLC musí být nahrán certifikát, který poskytne provozovatel DB serveru (nebo certifikát autority, na kterou se certifikát DB serveru odkazuje).

(DB nemůže ověřit totožnost PLC, klientské certifikáty zatím nepodporujeme.)

Komunikační scénáře

PLC se připojuje k e-mail serveru přes SMTP, chce odeslat mail



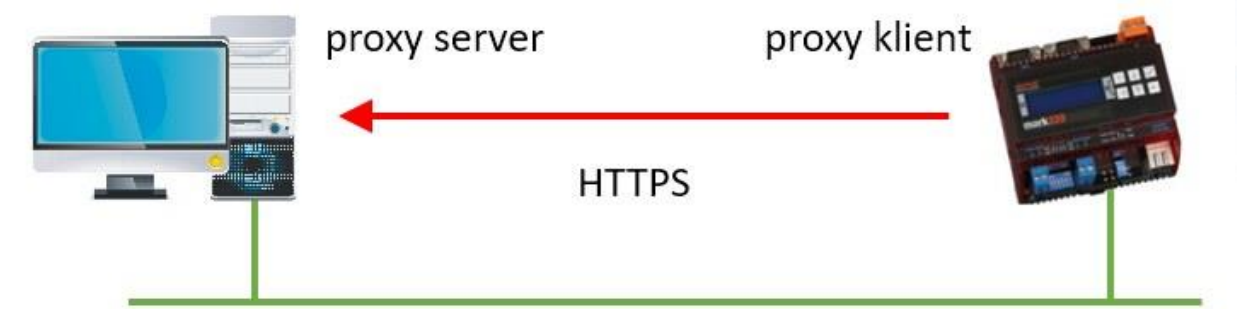
Bez zabezpečení - Server obvykle naslouchá na TCP portu 25.
Dnes je toto prakticky možné jen v lokálních sítích. Všechny veřejné servery již vyžadují zabezpečené spojení.

Zabezpečené spojení bez validace domény - Server obvykle používá TCP port 587 nebo 465. Pro nastavení stačí zaškrtnout "Povolit SSL" v definici alarmového kanálu. Do PLC není nutné nahrávat žádné certifikáty atd. Pouze šifrování.

Zabezpečené spojení s validací domény - Zaškrtne se "*Validace certifikátu*" v nastavení definic hlášení.
PLC se při navazování spojení ujistí, že mailový server je tím, za koho se prohlašuje (tedy že PLC se nepřipojuje na nějaký jiný, podvržený server). V PLC musí být v User CA nebo Default CA nahrán certifikát, který poskytne správce e-mailového serveru (nebo certifikát autority, na který se certifikát e-mail serveru odkazuje v rámci *řetězce důvěry*).

Komunikační scénáře

PLC se připojuje na Domat Proxy server



PLC je z TLS pohledu klient, ale z hlediska aplikačního je serverem!

Bez zabezpečení: Standardní http spojení. V PLC nastavíme Proxy **URL http://plcproxy.domat.cz:12349**

Zabezpečené, bez validace domény: Žádné certifikáty není nutné nahrávat. V PLC v nastavení proxy stačí zadat URL ve tvaru **https://plcproxy.domat.cz:12359** (pozor, číslo portu je jiné než u nezabezpečeného spojení).

S validací domény: V PLC musí být navíc nahrán certifikát, který poskytne správce proxy serveru (Domat). Ve výchozím stavu je v PLC doménový certifikát Domat již nahrán.

Komunikační scénáře

SSCP klient (IDE, PLC, SCADA) se připojuje na Domat Proxy server

Bez zabezpečení: Standardní SSCP spojení. V IDE v Parametrech připojení nastavíme Proxy URL **tcp://plcproxy.domat.cz:12348**

Zabezpečené, bez validace domény: Žádné certifikáty není nutné nahrávat. V IDE stačí zadat URL ve tvaru **tcps://plcproxy.domat.cz:12358** (pozor, číslo portu je jiné než u nezabezpečeného spojení).

S validací domény: V PC s klientem musí být navíc nahrán certifikát, který poskytne správce proxy serveru (dodá Domat).

(Možné všechny kombinace TLS / nonTLS, Proxy klient / SSCP klient)

Praktické aspekty nasazení

Kdo je odpovědný za bezpečnost? (dodavatel / provozovatel / ...)

- udržení know-how po předání systému
- otázky záruky a servisu

Certifikáty mají omezenou platnost – nutno pravidelně obnovovat:

- provozní náklady
- riziko nefunkčnosti systému „...samo od sebe“ (*časovaná bomba*) – viz log PLC
- kompetence na straně odpovědného subjektu (zálohy, lidé)

ISO 27001, ČSN EN IEC 62443-3-3, NIS2 atd.

Dotazy, diskuze...

Další zdroje: např. https://www.domat-int.com/cs/tls-zabezpeceni

Dotazy, diskuze

Děkuji za pozornost!

jan.vidim@domat.cz