



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)

Pokojevé ovladače a regulátory

DUC

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



* in black or white housing



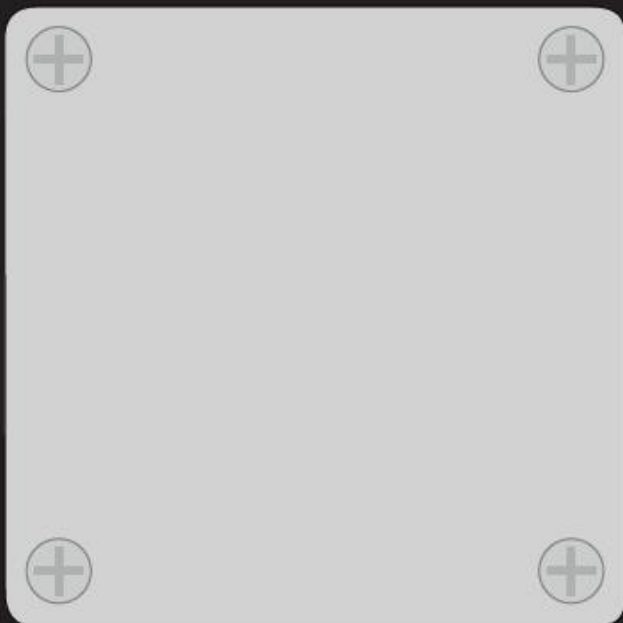
DUC219

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



* in black or white housing

Pokojové ovladače a regulátory



EPC103

heating / cooling controller for EPC projects
with external 1-Wire temperature sensor ST1W

2  DI, 2  DO SSR

24 V AC / DC

communicative



Pokojevé ovladače a regulátory



The image shows a black rectangular FCU controller unit, model DFCRO10, by domat. It features a terminal block at the top with orange and blue connectors. The front panel has labels for Tx1, PWR, Tx2, INIT, USR, BUS, END, K1+, K1-, K2+, and K2-. The unit is labeled 'DFCRO10' and 'domat CONTROL SYSTEM MADE IN CZECH REPUBLIC'. At the bottom, there are labels for D11, D12, G, G, S, S, D01, D02, COM, D1, D2, and D3.

DFCRO10

FCU controller
temperature regulation 
for use with *DUC* room unit
2  DI, 2  DO SSR, 3  DO relays
24 V AC / DC
communicative  

**Also as DFCRO11 for 230 V AC*

Pokojevé ovladače a regulátory

DFCRO13

FCU controller
temperature regulation
for use with *DUC* room unit
2 DI, 2 DO SSR, 3 AO 0..10 V
24 V AC / DC
communicative



The image shows a black rectangular control unit, the DFCRO13, with various terminals and labels. At the top, there are two rows of screw terminals: a yellow row on the left and a blue row on the right. Below these, the unit has labels for 'Tx1', 'PWR', 'Tx2', 'INIT', 'USR', 'BUS', 'END', 'K1+', 'K1-', 'K2+', and 'K2-'. The unit features a large 'DFCRO13' label and the 'domat CONTROL SYSTEM' logo. At the bottom, there are more terminals labeled 'DI1', 'DI2', 'DO1', 'DO2', 'G', 'G', 'G0', 'G0', 'G0', 'G0', 'AO1', 'AO2', and 'AO3'. The unit is designed for temperature regulation and communication via RS485 and Modbus.

Pokojevé ovladače a regulátory



The image shows a Domat DFCR015 VAV controller. It is a black rectangular unit with a terminal block at the top with orange and blue connectors. The front panel has labels for Tx1, PWR, Tx2, INIT, USB, BUS, END, K1+, K1-, K2+, and K2-. Below these are icons for a relay, a temperature sensor, and a CO2 sensor. The model name 'DFCR015' is prominently displayed in large white letters. Below it, the 'domat' logo is shown, followed by 'CONTROL SYSTEM' and 'MADE IN CZECH REPUBLIC'. At the bottom, there are labels for DI1, DI2, DO1, DO2, G, G, G0, G0, G0, A01, A02, and A03. The bottom of the unit features a multi-pin connector.

DFCR015

VAV controller
temperature & CO₂ regulation  
for use with *DUCCO2* room unit
2  DI, 2  DO SSR, 3  AO 0...10 V
24 V AC / DC
communicative  

Pokojevé 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

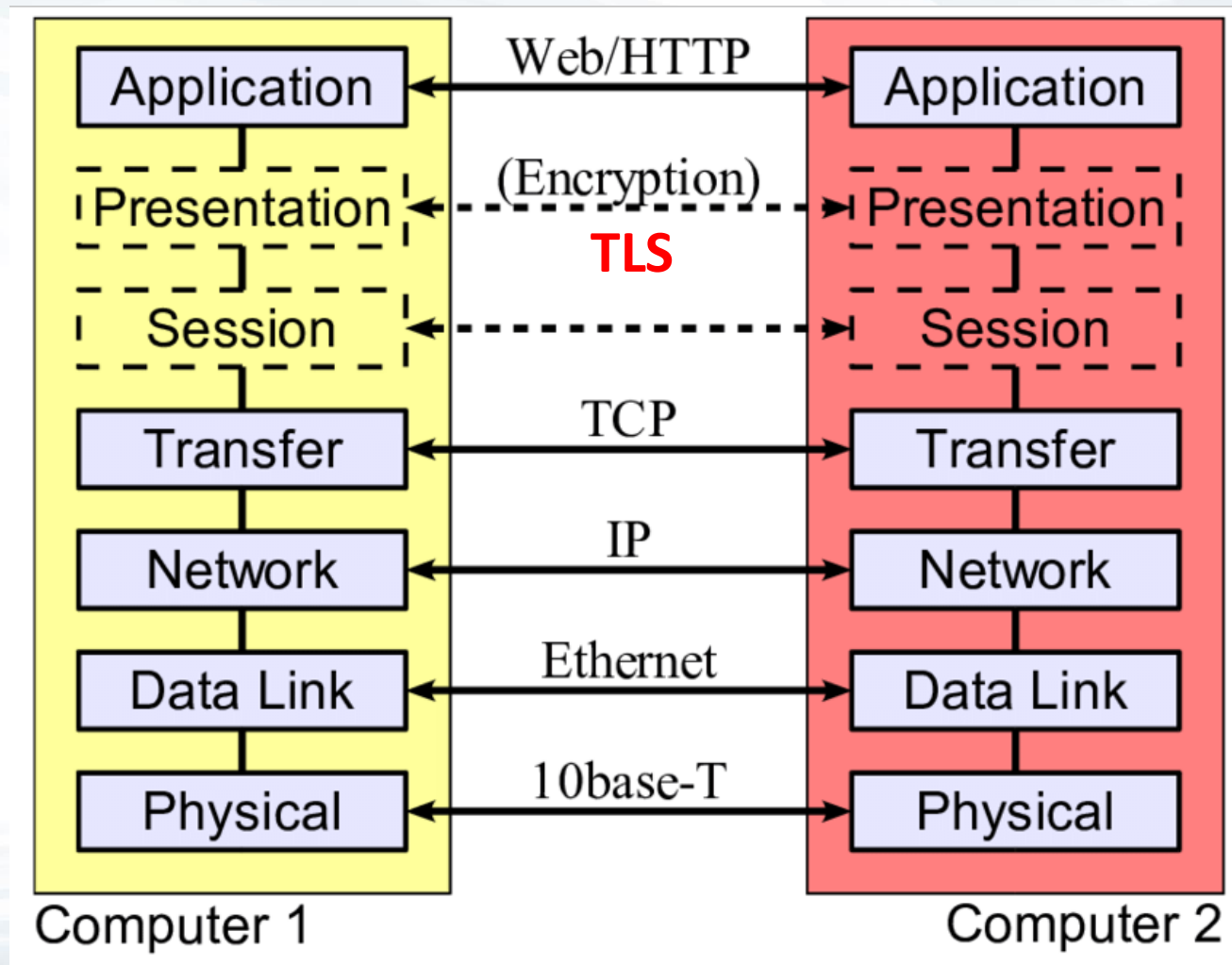
TLS

- 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

442 27.888047 192.168.1.24 213.160.171.74 HTTP 555 POST /login.cgi HTTP/1.1 (application/x-www-form-urlencoded)

443 27.888047 213.160.171.74 192.168.1.24 TCP 54 80 → 64723 [ACK] Seq=1 Ack=503 Win=2160 Len=0

444 27.888047 213.160.171.74 192.168.1.24 HTTP/JSON 317 HTTP/1.1 200 OK , JavaScript Object Notation (application/json)

> Frame 442: 555 bytes on wire (4440 bits), 555 bytes captured (4440 bits) on interface \\Device\\NPF_{0894A...}

> Ethernet II, Src: IntelCor_96:83:90 (00:28:f8:96:83:90), Dst: HTC_8f:e7:1f (00:ee:bd:8f:e7:1f)

> Internet Protocol Version 4, Src: 192.168.1.24, Dst: 213.160.171.74

> Transmission Control Protocol, Src Port: 64723, Dst Port: 80, Seq: 2, Ack: 1, Len: 501

> Hypertext Transfer Protocol

> POST /login.cgi HTTP/1.1\\r\\n

Host: 213.160.171.74\\r\\n

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/119.0\\r\\n

Accept: application/json, text/plain, */*\\r\\n

Accept-Language: cs,sk;q=0.8,en-US;q=0.5,en;q=0.3\\r\\n

Accept-Encoding: gzip, deflate\\r\\n

Content-Type: application/x-www-form-urlencoded\\r\\n

> Content-Length: 66\\r\\n

Origin: http://213.160.171.74\\r\\n

DNT: 1\\r\\n

Connection: keep-alive\\r\\n

Referer: http://213.160.171.74/\\r\\n

[Full request URI: http://213.160.171.74/login.cgi]

[HTTP request 1/1]

[Response in frame: 444]

File Data: 66 bytes

> HTML Form URL Encoded: application/x-www-form-urlencoded

> Form item: \"{\\\"ver\\\":1,\\\"c\\\":{\\\"u\\\":\\\"admin\\\",\\\"p\\\":\\\"3b17ac03d64b318172264b801bc6098a\\\"}}\" = \"\"

Key: {\\\"ver\\\":1,\\\"c\\\":{\\\"u\\\":\\\"admin\\\",\\\"p\\\":\\\"3b17ac03d64b318172264b801bc6098a\\\"}}

Value:

0030 00 fe d5 6c 00 00 50 4f 53 54 20 2f 6c 6f 67 69 ...1..PO ST /logi

0040 6e 2e 63 67 69 20 48 54 54 50 2f 31 2e 31 0d 0a n.cgi HT TP/1.1..

0050 48 6f 73 74 3a 20 32 31 33 2e 31 36 30 2e 31 37 Host: 21 3.160.17

0060 31 2e 37 34 0d 0a 55 73 65 72 2d 41 67 65 6e 74 1.74..Us er-Agent

0070 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 : Mozill a/5.0 (W

0080 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 3b 20 indows N T 10.0;

0090 57 69 6e 36 34 3b 20 78 36 34 3b 20 72 76 3a 31 Win64; x 64; rv:1

00a0 30 39 2e 30 29 20 47 65 63 6b 6f 2f 32 30 31 30 09.0) Ge cko/2010

00b0 30 31 30 31 20 46 69 72 65 66 6f 78 2f 31 31 39 0101 Fir efox/119

00c0 2e 30 0d 0a 41 63 63 65 70 74 3a 20 61 70 70 6c .0..Acce pt: appl

00d0 69 63 61 74 69 6f 6e 2f 6a 73 6f 6e 2c 20 74 65 ication/ json, te

00e0 78 74 2f 70 6c 61 69 6e 2c 20 2a 2f 2a 0d 0a 41 xt/plain , */*..A

00f0 63 63 65 70 74 2d 4c 61 6e 67 75 61 67 65 3a 20 ccept-La nguage:

0100 63 73 2c 73 6b 3b 71 3d 30 2e 38 2c 65 6e 2d 55 cs,sk;q= 0.8,en-U

0110 53 3b 71 3d 30 2e 35 2c 65 6e 3b 71 3d 30 2e 33 S;q=0.5, en;q=0.3

0120 0d 0a 41 63 63 65 70 74 2d 45 6e 63 6f 64 69 6e ..Accept -Encodin

0130 67 3a 20 67 7a 69 70 2c 20 64 65 66 6c 61 74 65 g: gzip, deflate

0140 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 ..Conten t-Type:

0150 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 2d 77 77 applicat ion/x-ww

0160 77 2d 66 6f 72 6d 2d 75 72 6c 65 6e 63 6f 64 65 w-form-u rlencode

0170 64 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 d..Conte nt-Lengt

0180 68 3a 20 36 36 0d 0a 4f 72 69 67 69 6e 3a 20 68 h: 66..O rigin: h

0190 74 74 70 3a 2f 2f 32 31 33 2e 31 36 30 2e 31 37 ttp://21 3.160.17

01a0 31 2e 37 34 0d 0a 44 4e 54 3a 20 31 0d 0a 43 6f 1.74..DN T: 1..Co

01b0 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 nnection : keep-a

01c0 6c 69 76 65 0d 0a 52 65 66 65 72 65 72 3a 20 68 live..Re ferer: h

01d0 74 74 70 3a 2f 2f 32 31 33 2e 31 36 30 2e 31 37 ttp://21 3.160.17

01e0 31 2e 37 34 2f 0d 0a 0d 0a 7b 22 76 65 72 22 3a 1.74/... -{\\\"ver\\\":

01f0 31 2c 22 63 22 3a 7b 22 75 22 3a 22 61 64 6d 69 1,\\\"c\\\":{\\\" u\\\":\\\"admi

0200 6e 22 2c 22 70 22 3a 22 33 62 31 37 61 63 30 33 n\\\",\\\"p\\\":\\\" 3b17ac03

0210 64 36 34 62 33 31 38 31 37 32 32 36 34 62 38 30 d64b3181 72264b80

0220 31 62 63 36 30 39 38 61 22 7d 7d 1bc6098a \"}}}

TLS

V programu Wireshark:

Ethernet

IP

TCP

TLS

432 16.238968 192.168.1.100 77.236.192.210 TCP 54 64107 → 443 [ACK] Seq=2648 Ack=1692 Win=131328 Len=0

433 16.239091 192.168.1.100 77.236.192.210 TLSv1.3 78 Application Data

434 16.239132 192.168.1.100 77.236.192.210 TCP 54 64107 → 443 [FIN, ACK] Seq=2672 Ack=1692 Win=131328 Len=0

> Frame 433: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface \Device\NPF_{0894A520-...}

> Ethernet II, Src: IntelCor_96:83:90 (00:28:f8:96:83:90), Dst: Routerbo_83:15:49 (78:9a:18:83:15:49)

> Internet Protocol Version 4, Src: 192.168.1.100, Dst: 77.236.192.210

> Transmission Control Protocol, Src Port: 64107, Dst Port: 443, Seq: 2648, Ack: 1692, Len: 24

▼ Transport Layer Security

▼ TLSv1.3 Record Layer: Application Data Protocol: Hypertext Transfer Protocol

Opaque Type: Application Data (23)

Version: TLS 1.2 (0x0303)

Length: 19

Encrypted Application Data: e2513294f9eda2fab4f51037fb784b651b469f

[Application Data Protocol: Hypertext Transfer Protocol]

0000 78 9a 18 83 15 49 00 28 f8 96 83 90 08 00 45 00 x...I.(.....E.

0010 00 40 17 fc 40 00 80 06 11 f1 c0 a8 01 64 4d ec .@.@... ..dM.

0020 c0 d2 fa 6b 01 bb 4a 4a 50 58 5e 6f 04 90 50 18 ...k..JJ PX^o..P.

0030 02 01 95 a4 00 00 17 03 03 00 13 e2 51 32 94 f9Q2...

0040 ed a2 fa b4 f5 10 37 fb 78 4b 65 1b 46 9f7. xKe.F.

Transport Layer Security (tls), 24 byte(s)

Packets: 472 · Displayed: 472 (100.0%) · Dropped: 0 (0.0%)

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

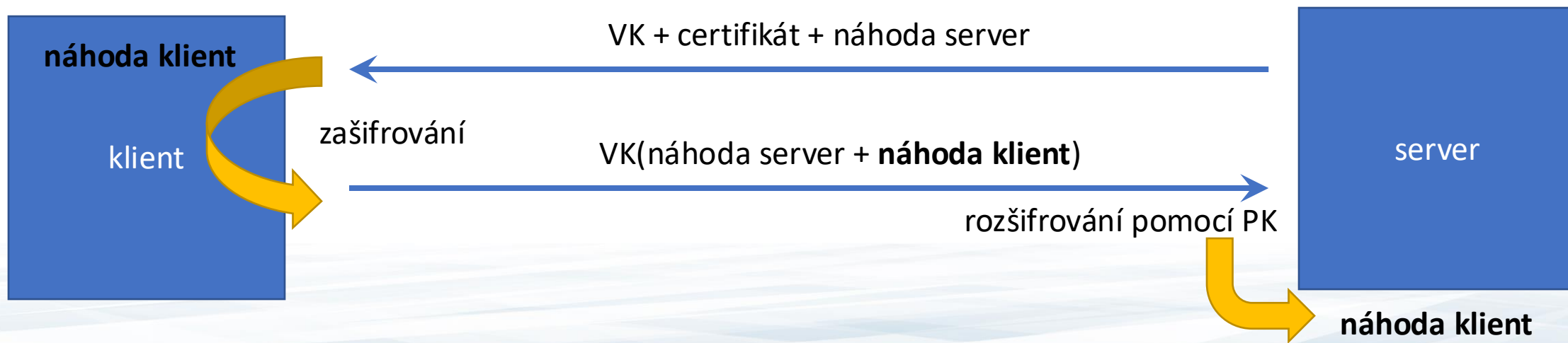
Postup:

- 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. clientský 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 informace o tom, co je server zač.

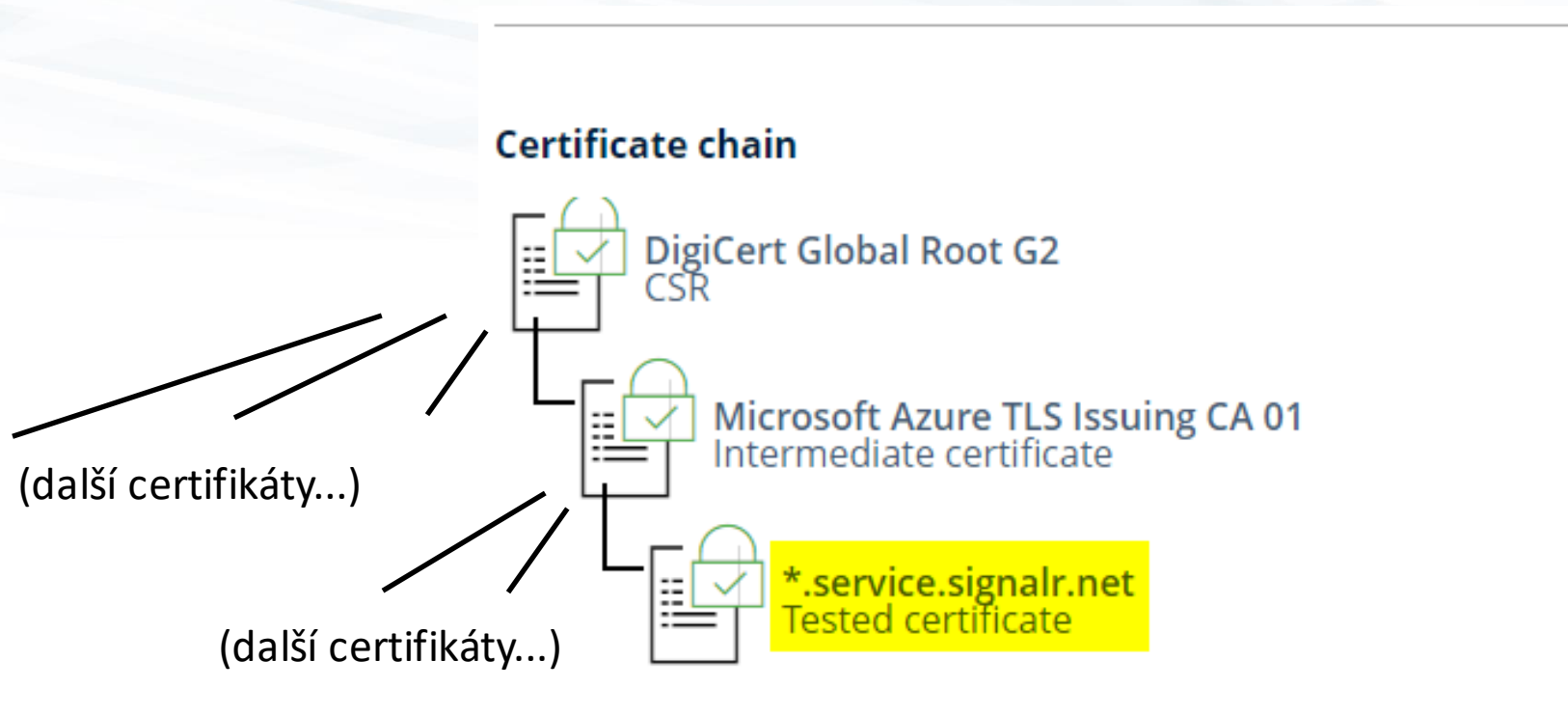
Klient ho ověřuje proti (stejnému) certifikátu, který má (nebo proti *řetězci důvěry*).

- **self-signed** – certifikát podepsaný sám sebou („vizitka“), klient ho
 - buď akceptuje bez dalších pochyb, což je případ spojení **bez validace certifikátu**,
 - nebo porovná s tímtež 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 nahran u klienta v **user_ca**. Pokud je certifikát nahran 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 nahran u klienta v adresáři s certifikáty standardních autorit **user_ca**. Operační systém Windows obvykle základní (kořenové) certifikáty obsahuje, jinak je lze nainstalovat.

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)

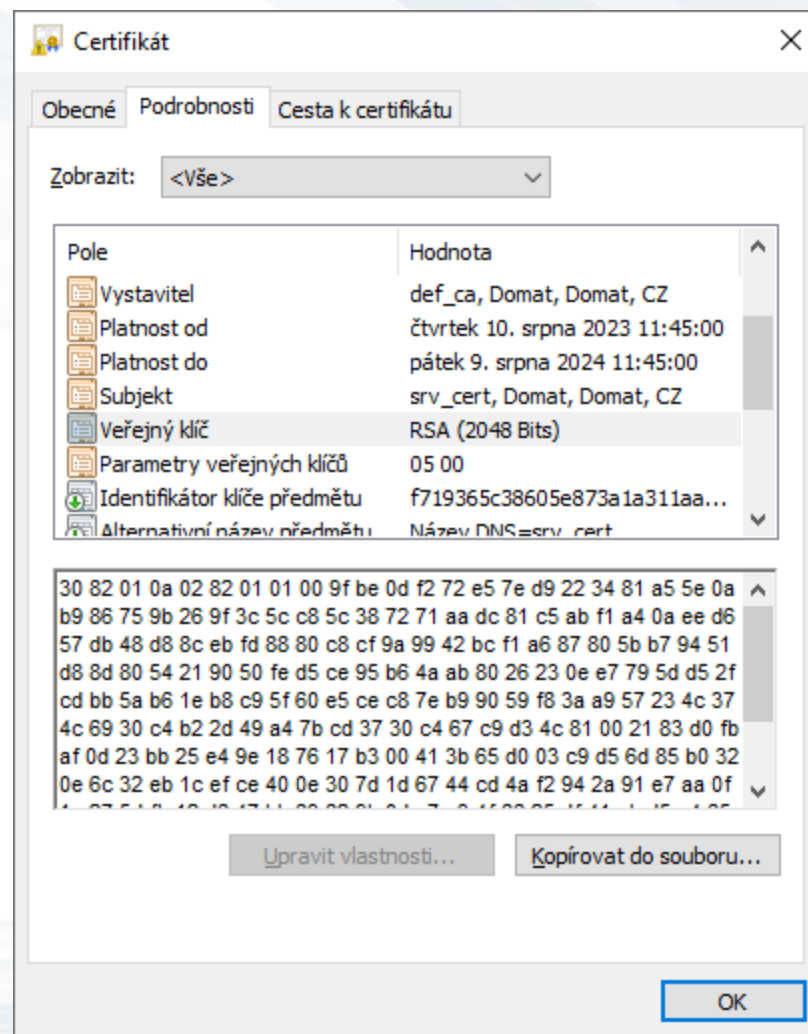
Součástí certifikátu je i veřejný klíč (aby protistrana mohla zasílat šifrované zprávy).

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

Certifikát

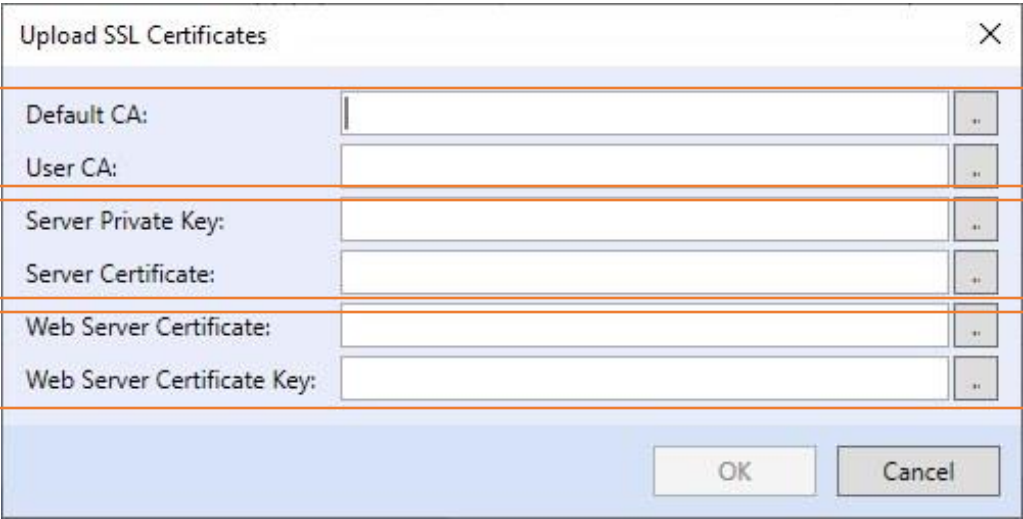
Jak vypadá?

```
domat_server_cert.crt
1 -----BEGIN CERTIFICATE-----
2 MIIDoTCCAomgAwIBAgIIRX65y+Pes+MwDQYJKoZIhvcNAQELBQAwPjELMAkGA1UE
3 BhMCQ1oxDjAMBgNVBAoTBURvbWF0MQ4wDAYDVQQLEwVEb21hdDEPMA0GA1UEAwwG
4 ZGVmX2NhMB4XDTEzMDgxMDEwNDUwMFOxDTIOMDgwOTEwNDUwMFOwQDELMAkGA1UE
5 BhMCQ1oxDjAMBgNVBAoTBURvbWF0MQ4wDAYDVQQLEwVEb21hdDERMA8GA1UEAwwI
6 c3J2X2N1cnQwgGElMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCfvg3ycuV+
7 2SI0gaVeCrmGdZsmnzxcyFw4cnGq3IHFq/GkCu7WV9tI2Izr/YiAyM+amUK88aaH
8 gFu3lFHYjYBUIZBQ/tX0lbZKq4AmIw7neV3VL827WrYeuMlfYOXOyH65kFn4Oq1X
9 I0w3TGkwXLIItSaR7zTcwXGfJ00yBACGD0PuvDSO7JeSeGHYXswBBO2XQA8nVbYWw
10 Mg5sMusc785ADjB9HWdEzUrylCqR56oPGidd+XLWR7tjYpsN58NPacXfQavVpGVe
11 sq5rB8aXjevW6Q7qDqv8VsqiciVqsyPXcdYmSCP7LU64f0YKRpeBGCWEYqCkwSmz
12 lbDerOrSWNaLAGMBAAGjgaAwgZ0wDAYDVR0TAQH/BAIwADAdBgNVHQ4EFgQU9xk2
13 XDhgXoc6GjEaobxg3JJQgpIwDgYDVR0PAQH/BAQDAgPoMBYGA1UdJQEB/wQMMAoG
14 CCsGAQUFBwMBMBMGAlUEQQMMAqCCHNydl9jZXJ0MBEGCWCWSAGG+EIBAQQEAWIG
15 QDAeBg1ghkgBhvCAQ0EERYPeGNhIGN1cnRpZmljYXR1MA0GCSqGSIb3DQEBCwUA
16 A4IBAQCmnIPdqW4ccoaefFf3buyv3DcIMG4ipyRxW6Egk9KCCgtC8rk0VCN1juuA
17 64wD10JE5HG9bSgumq69EKOFYmGT5d6t6S79A6gvlHbICAGE4YSP3pausKOrtIoH
18 ALe8ISz8khzwwWLVITBjCRlZRWCD0/QHR8rTCAX4U4sRImtSlbI5LqFlgScX7jWd
19 pYHdeM0bBlbrIqkLI/nwElMOidUHJAajKffSNXI40p7xElssFhJxGhBjProig7/s
20 ysKNj5/IJO8Wdm6azAI9MhWknP9DZ3jtr3wsS2qsMoHXOo6s9qfWVIVbRvhdUwO6
21 8iG7cnakGuBrvzCnbvEl/RxYE5bS
22 -----END CERTIFICATE-----
23
```



Nahrávání do PLC

PLC – Operace s PLC – Nahrání certifikátů



Pro Proxy server a Merbon DB (PLC je klientem)

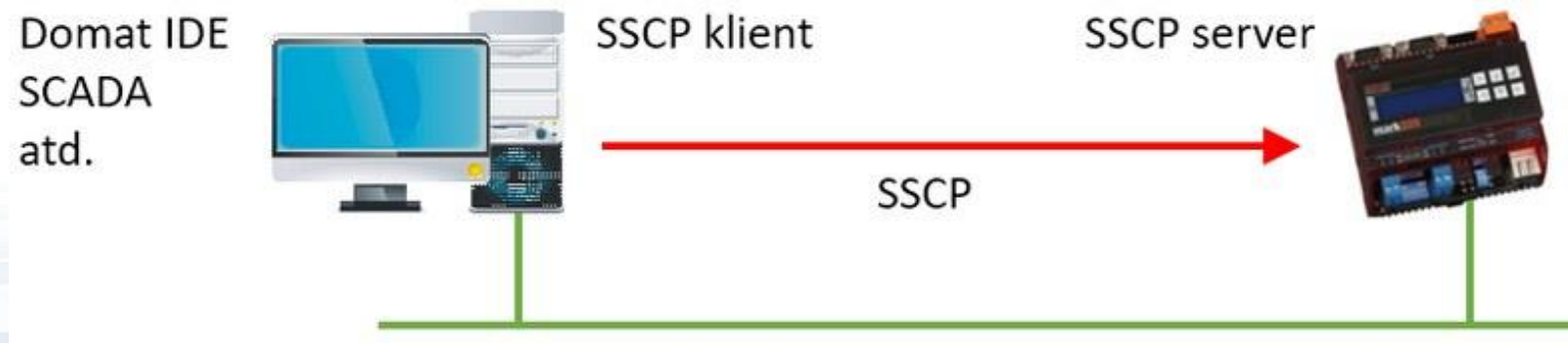
Pro SSCP server: certifikát + privátní klíč

Pro webový přístup: certifikát + privátní klíč

Nahrávání do PLC

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

Server Private Key:		B1	Pro SSCP server
Server Certificate:		B1	
Web Server Certificate:		B1	Pro webový přístup
Web Server Certificate Key:		B1	

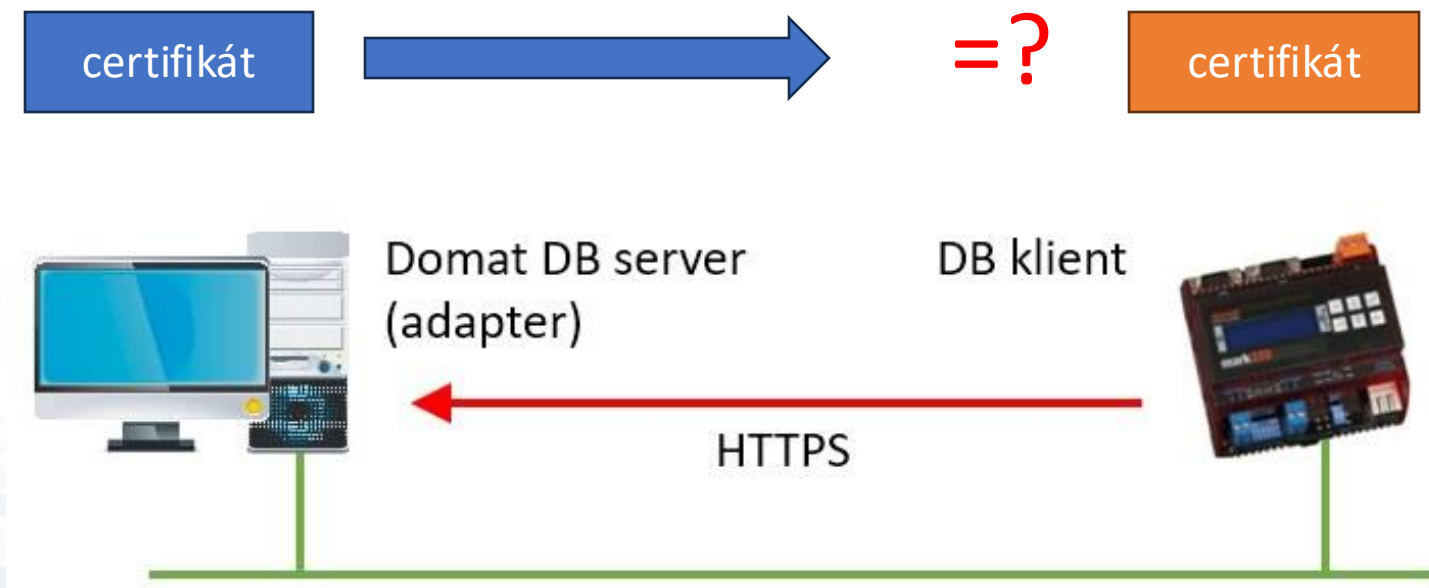


Nahrávání do PLC

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

Default CA:		OK
User CA:		OK

Pro Proxy server a Merbon DB (PLC je klientem)



Nahrávání do PLC

Jaké certifikáty a klíče jsou nahrány z výroby?

The screenshot shows a dialog box titled "Upload SSL Certificates" with a close button (X) in the top right corner. It contains six input fields, each with a "Browse" button (represented by a small icon with "B" and a magnifying glass) to its right. The fields are labeled as follows: "Default CA:", "User CA:", "Server Private Key:", "Server Certificate:", "Web Server Certificate:", and "Web Server Certificate Key:". At the bottom of the dialog are "OK" and "Cancel" buttons. Five blue arrows originate from the text on the right and point to the following fields: 1. From "Výchozí CA" to "Default CA:". 2. From "Uživatelská CA" to "User CA:". 3. From "Privátní klíč serveru" to "Server Private Key:". 4. From "Serverový certifikát" to "Server Certificate:". 5. From "Web server certificate a Web server certificate key" to "Web Server Certificate Key:".

- 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 nahráný v *user_ca* - toto si zařídí uživatel, který buduje vlastní systém důvěry.

Komunikační scénáře

Webový prohlížeč se připojuje pomocí https:// na PLC



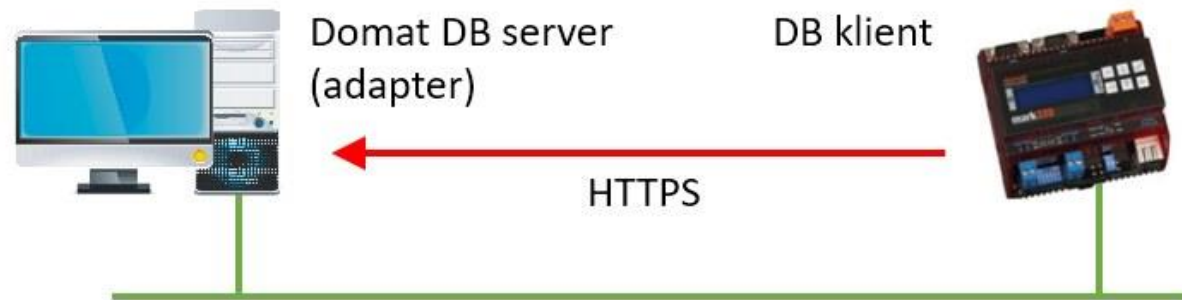
Bez zabezpečení - Spojení přes protokol *http://* (TCP port 80). Některé prohlížeče již umožňují přístup jen v místní síti, ne přes Internet; nutno odsouhlasit, že uživatel přistupuje na nezabezpečený web.

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.

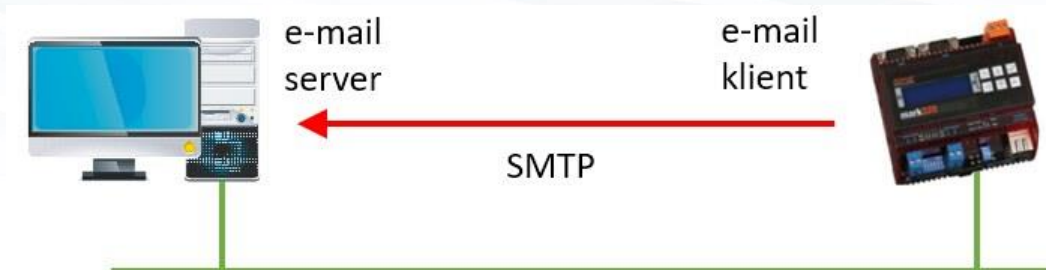
Zabezpečené spojení bez validace domény: Zabezpečené spojení, v PLC stačí zadat URL ve tvaru *https://*. Do PLC není nutné nahrávat žádné certifikáty, klíče atd.

Zabezpečené spojení s validací domény: V PLC musí být nahrán certifikát, který poskytne provozovatel DB serveru (nebo certifikát authority, 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 - Zaškrtně 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>



The screenshot shows the website of domat, a member of ČEZ ESCO. The header includes the company logo, a search bar, and a navigation menu with links: O NÁS, SYSTÉM, PRODUKTY, SLUŽBY, REFERENCE, KE STAŽENÍ, and KONTAKTY. The main content area is titled 'FAQ a technická podpora' and 'TLS zabezpečení'. The article 'TLS ZABEZPEČENÍ' discusses the importance of secure communication in PLC systems, mentioning Transport Layer Security (TLS) and its application in project design and programming. It also provides links to general TLS information and communication examples.

domat
ČLEN ČEZ ESCO

Zadejte hledaný výraz

O NÁS | SYSTÉM | PRODUKTY | SLUŽBY | REFERENCE | KE STAŽENÍ | KONTAKTY

FAQ a technická podpora | TLS zabezpečení

TLS ZABEZPEČENÍ

Zabezpečená komunikace u PLC rychle nabývá na významu a u některých projektů je nasazení PLC s TLS (**Transport Layer Security**) zabezpečením již podmínkou. V následujícím textu se seznámíme se základy šifrování a ověřování a ukážeme si některé scénáře z hlediska projektování a aplikačního programování. Více informací k celé problematice, podrobnější popisy navazování spojení a podobně jsou k nalezení na Internetu, zde se budeme věnovat jen základním principům a zejména dopadům na organizaci projektu a nastavení PLC a dalších programů. Někdy se setkáme se zkratkou SSL (Secure Socket Layer), TLS je její modernější nástupce.

- TLS zabezpečení – obecně
- TLS zabezpečení – příklady komunikací

Dotazy, diskuze

Děkuji za pozornost!

jan.vidim@domat.cz

Energie pod kontrolou