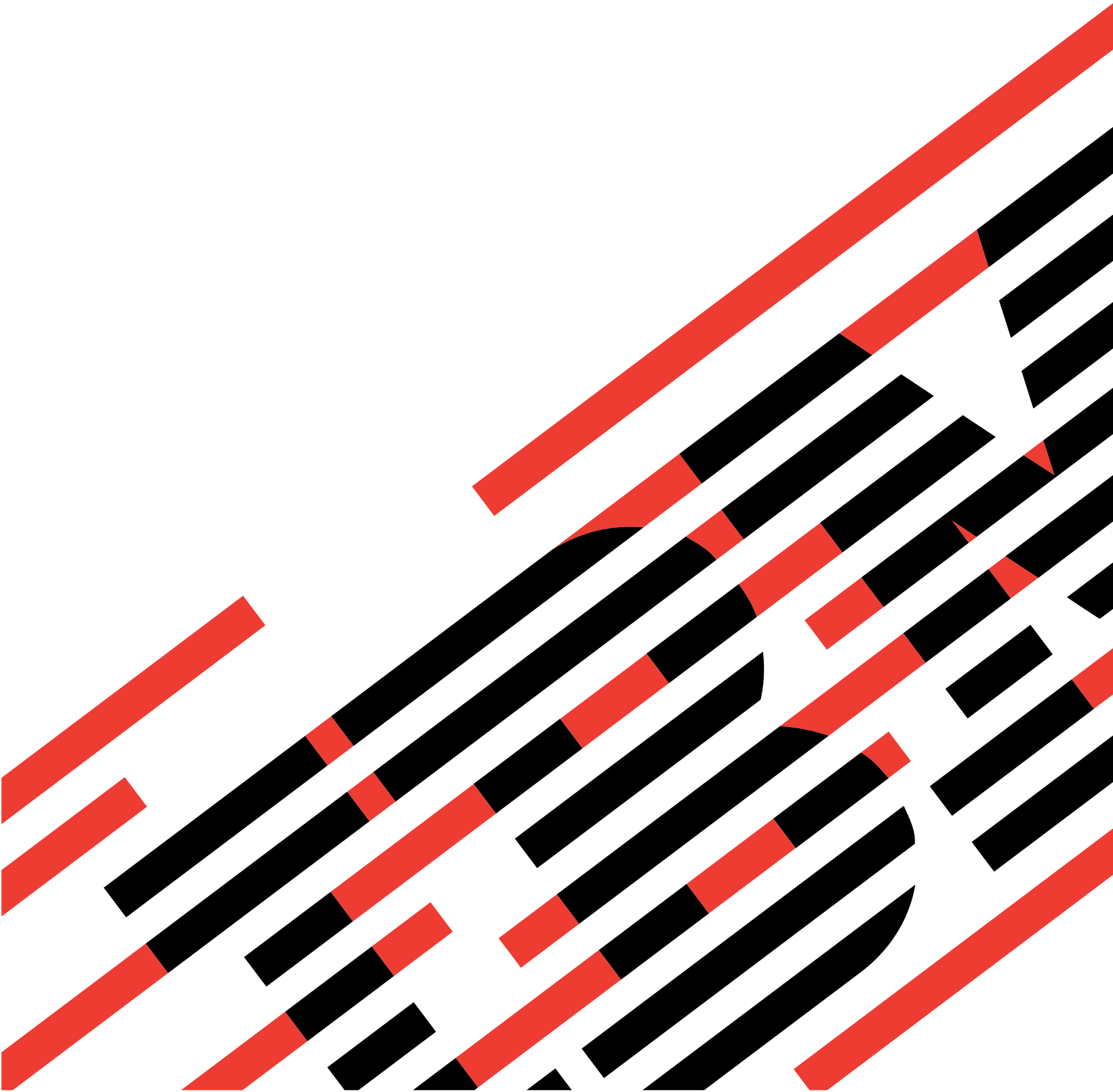
IBM

eserver

iSeries

# SSL (Secure Sockets Layer)



IBM

@server

iSeries

# SSL (Secure Sockets Layer)

# Obsah

# Část 1. SSL (Secure Sockets Layer)

iSeries SSL (Secure Sockets Layer) je v současné době odvětvovým standardem podporujícím aplikace pro zabezpečení komunikačních relací v nechráněné síti, jako je například Internet. Více informací o SSL a aplikacích serveru iSeries najdete v těchto částech:

- **Co je nového ve verzi V5R2**
  Tato část popisuje nové funkce a nové informace týkající se SSL.
- **Scénáře SSL**
  Tato část obsahuje nové dodatky k informacím o SSL a pomocí příkladů ilustrujících, jak funguje SSL, pomáhá lépe pochopit funkci SSL na serveru iSeries.
- **Koncepce SSL**
  Tato část zahrnuje dodatečné informace, které popisují některé stavební kameny protokolů SSL.
- **Plánování umožnění SSL**
  Tato část popisuje nezbytné předpoklady pro umožnění SSL na serveru iSeries a uvádí několik užitečných rad.
- **Zabezpečení aplikací pomocí SSL**
  Tato část zahrnuje seznam aplikací, které můžete zabezpečit pomocí SSL na serveru iSeries.
- **Odstraňování problémů s SSL**
  Tato část nabízí základního průvodce procedurou odstraňování problémů se SSL na serveru iSeries.
- **Související informace pro SSL**
  Tato část zahrnuje odkazy na další zdroje informací.

# Kapitola 1. Co je nového ve verzi V5R2

2058 Cryptographic Accelerator pro server iSeries představuje volbu dostupnou ve V5R2M0. Tato volba šifrovacího hardwaru je navržena pro zlepšení výkonu SSL na serveru iSeries. Více informací o této volbě najdete pod tématem zabývajícím se šifrovacím hardwarem.

**Nové rozhraní GSKit API (Global Secure Kit application programming interface)**

K dispozici je nové rozhraní OS/400 GSKit API (Global Secure Toolkit): gsk_secure_soc_startInit(). Více informací najdete pod tématem KSKit API (Global Secure ToolKit).

Další informace o tom, co bylo změněno nebo co je nového v tomto vydání, uvádí téma Sdělení pro uživatele.

**Jak zjistit, co je nového nebo co se změnilo**

Za účelem snadnější identifikace míst, kde byly provedeny technické změny, jsou tyto informace označeny symbolem

- Symbol

  označuje, kde začínají nové nebo změněné informace.
- Symbol « označuje, kde nové nebo změněné informace končí.

# Kapitola 2. Tisk tohoto tématu

Můžete si prohlédnout nebo stáhnout tyto informace ve formátu PDF. Pokud tak chcete učinit, vyberte téma Zabezpečení aplikací pomocí SSL (přibližně 215 KB nebo 34 stran).

### Další informace

Můžete si také prohlédnout nebo vytisknout jakékoliv ze souvisejících informací vztahujících se k tomuto tématu.

### Jak uložit soubory ve formátu PDF

Chcete-li soubory ve formátu PDF uložit na pracovní stanici za účelem prohlížení nebo tisku:
1. Klepněte v prohlížeči pravým tlačítkem myši na PDF.
2. Klepněte na **Save Target As** (Uložit jako).
3. Navigujte do adresáře, kam chcete PDF uložit.
4. Klepněte na **Save** (Uložit).

### Jak stáhnout program Adobe Acrobat Reader

Jestliže potřebujete aplikaci Adobe Acrobat Reader, abyste si mohli prohlédnout nebo vytisknout tyto informace, můžete si jeho kopii stáhnout na webové stránce společnosti Adobe na adrese

www.adobe.com/products/acrobat/readstep.html. 

# Kapitola 3. Scénáře SSL

Pro maximalizaci výhod aktivace SSL na serveru iSeries byly navrženy tyto scénáře:

- Scénář: Zabezpečení produktu Centrální správa pomocí SSL.
- Scénář: Zabezpečení FTP pomocí SSL.
- Scénář: Zabezpečení Telnet pomocí SSL.
- Scénář: Zvýšení výkonu iSeries SSL.
- Scénář: Ochrana privátních klíčů pomocí šifrovacího hardwaru.

## Scénář SSL: Zabezpečení produktu Centrální správa pomocí SSL

### Situace

Společnost právě instalovala síť WAN (wide area network), která zahrnuje několik serverů iSeries na vzdálených místech (koncové systémy), jenž jsou centrálně spravovány jedním serverem iSeries umístěným v hlavní kanceláři. Tom, specialista společnosti na zabezpečení ochrany dat, používá technologii produktu Centrální správa svého klienta iSeries Navigator, aby se připojil k serveru iSeries v hlavní kanceláři (centrální systém). Tom chce zabezpečit spojení mezi centrálním systémem a všemi koncovými servery pomocí SSL.

### Podrobnosti

Pomocí technologie produktu Centrální správa může Tom spravovat několik systémů prostřednictvím jednoho centrálního systému. Když bude Tom s produktem Centrální správa používat SSL, může tyto systémy spravovat **bezpečně**. Aby Tom mohl používat SSL s produktem Centrální správa, musí na PC, ze kterého spouští produkt Centrální správa, zabezpečit produkty iSeries Access for Windows a iSeries Navigator.

V prostředí produktu Centrální správa má Tom dvě úrovně autentizace:

**Autentizace serveru**
Umožňuje autentizaci certifikátu serveru koncového systému. Při připojování ke koncovému systému pracuje centrální systém jako klient SSL. Koncový systém se chová jako server SSL a musí prokázat svou identitu pomocí certifikátu, který byl vydán vydavatelem certifikátu (CA), jemuž centrální systém věří. Pro každý koncový systém musí vydavatel certifikátu (CA) vydat platný certifikát.

**Autentizace klienta a serveru**
Umožňuje autentizaci jak certifikátu centrálního systému, tak certifikátu koncového systému. Je pokládán za vyšší úroveň zabezpečení než úroveň autentizace serveru. V jiných aplikacích je tato autentizace známá jako autentizace klienta, kde klient musí poskytnout platný a důvěryhodný certifikát. Když se centrální systém (klient SSL) pokouší vytvořit spojení s koncovým systémem (server SSL), centrální systém a koncový systém si navzájem autentizují certifikáty kvůli pravosti vydavatele certifikátu (CA).

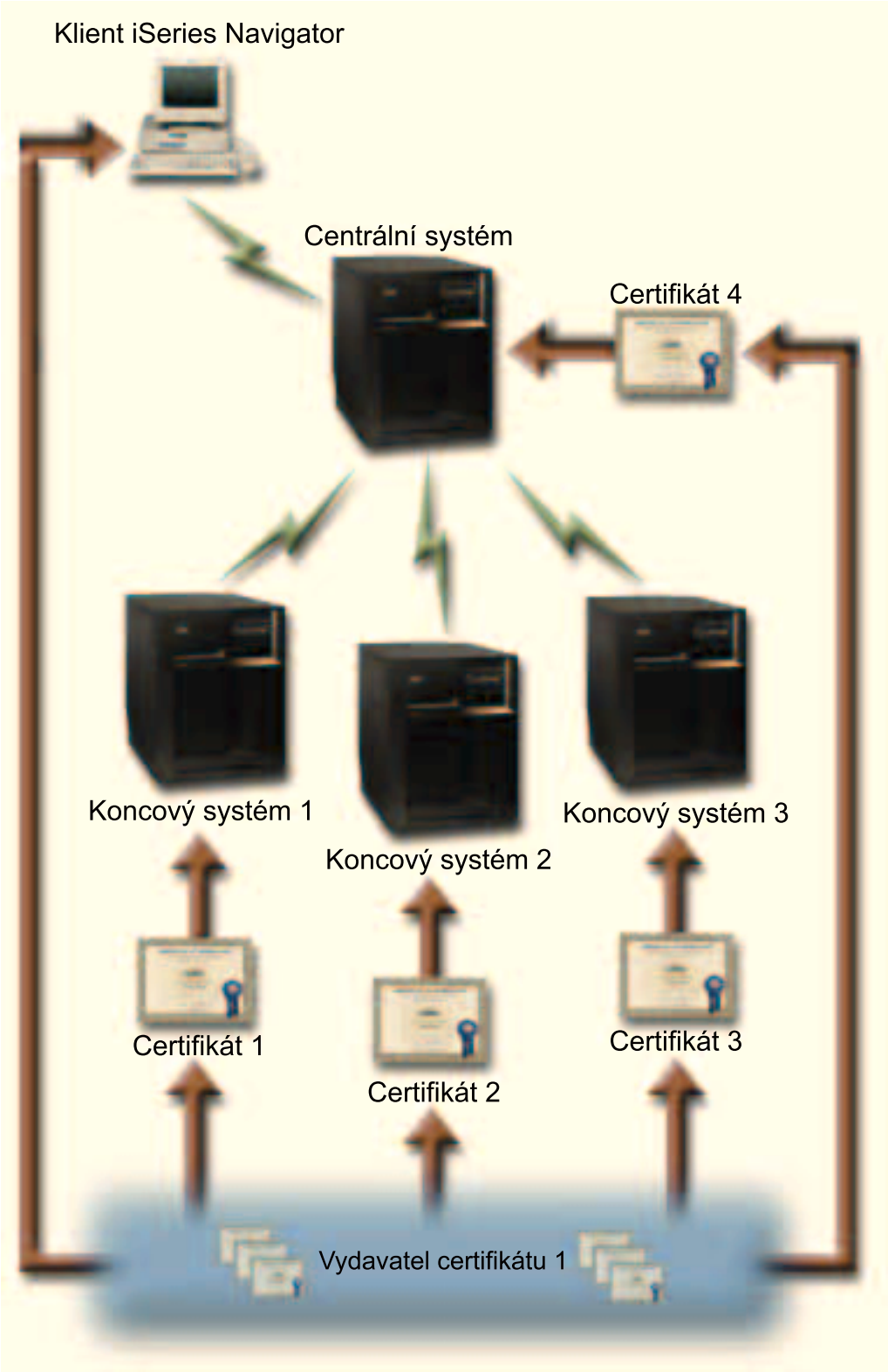
Na rozdíl od jiných aplikací poskytuje produkt Centrální správa autentizaci také prostřednictvím ověřovacího seznamu, který se nazývá důvěryhodná skupina. Obecně se dá říci, že ověřovací

- seznam obsahuje informace identifikující uživatele, jako je identifikace uživatele, a informace o autentizaci, jako je heslo, osobní identifikační číslo nebo digitální certifikát. Tyto informace o autentizaci jsou zakódovány.

Většina aplikací obvykle neuvádí aktivaci autentizace jak serveru, tak klienta. Je to kvůli tomu, že k autentizaci serveru dochází téměř vždy při aktivaci relace SSL. Mnoho aplikací má volby pro konfiguraci autentizace klienta. Produkt Centrální správa používá namísto termínu autentizace klienta termín ″autentizace serveru a klienta″ kvůli dvojí úloze, kterou má centrální systém v síti. Když se uživatelé PC připojují k centrálnímu systému a je aktivován SSL, centrální systém pracuje jako server. Když se však centrální systém připojuje ke koncovému systému, chová se jako klient. Níže uvedený obrázek ukazuje, jak centrální systém funguje v síti jako server i jako klient.

**Poznámka:** V případě zobrazeném na tomto obrázku musí být certifikát asociovaný s vydavatelem certifikátu (CA) uložen v databázi klíčů v centrálním systému a ve všech koncových

systémech.




**Nezbytné předpoklady**

Tom musí níže uvedené administrativní úlohy a úlohy konfigurace (viz obrázek Síť WAN Centrální správy zabezpečená pomocí SSL), aby produkt Centrální správa podporující SSL řádně fungoval:

1. Server iSeries používaný s produktem Centrální správa splňuje nezbytné předpoklady pro SSL (viz Nezbytné předpoklady pro SSL).
2. Server centrálního systému a všechny koncové servery iSeries používají verzi V5R2 operačního systému OS/400. Pokud používají verzi V5R1, nainstalujte níže uvedená PTF pro operační systém OS/400 (5722-SS1):
   a. SI01375
   b. SI01376
   c. SI01377
   d. SI01378
   e. SI01838
3. PC klient iSeries Navigator používá verzi V5R2 produktu iSeries Access for Windows. Používá-li klient verzi V5R1, nainstalujte servisní balík PTF SI01907 (nebo novější) pro verzi V5R1 iSeries Access for Windows (5722-XE1). Více informací najdete v rámci aplikace Information Center V5R1 pod tématem ″Securing Management Central″.
4. Získání vydavatele certifikátu (CA) pro servery iSeries.
5. Vytvoření certifikátu podepsaného vydavatelem certifikátu (CA) pro každý server iSeries, který má být spravován serverem Centrální správy podporujícím SSL.
6. Odeslání CA a certifikátu na každý server iSeries a jejich import do databáze klíčů.
7. Přiřazení certifikátů pomocí identifikace aplikací v rámci produktu Centrální správa a identifikace aplikací pro všechny koncové servery, které používají produkt iSeries Navigator:
   a. Spusťte na centrálním serveru produkt IBM DCM (Digital Certificate Manager). Pokud chce Tom získat nebo vytvořit certifikáty či jinak nastavit nebo změnit certifikační systém, provede to nyní (informace o nastavení certifikačního systému najdete pod tématem Použití produktu DCM (Digital Certificate Manager)).
   b. Klepněte myší na **Vybrat paměť certifikátů**.
   c. Vyberte ***SYSTEM** a klepněte myší na **Pokračovat**.
   d. Zadejte *SYSTEM **Heslo paměti certifikátů** a klepněte myší na **Pokračovat**. Jakmile se znovu načte menu, rozbalte volbu **Spravovat aplikace**.
   e. Klepněte myší na volbu **Aktualizace přiřazení certifikátu**.
   f. Vyberte volbu **Server** a klepněte myší na **Pokračovat**.
   g. Vyberte volbu **Server Centrální správy** a klepněte myší na volbu **Aktualizace přiřazení certifikátu**. Tím přiřadíte certifikát serveru k produktu Centrální správa, aby se vytvořila identita pro klienty iSeries Access for Windows.
   h. Klepněte myší na volbu **Přiřazení nového certifikátu**. Produkt DCM se znovu zavede na stranu **Aktualizace přiřazení certifikátu** se zprávou o potvrzení.
   i. Klepněte myší na **Provedeno**.
   j. Opakujte tuto proceduru pro všechny koncové servery, které používají produkt iSeries Navigator.
8. Nastavte produkt iSeries Navigator:
   a. Selektivně nainstalujte komponentu SSL pro produkt iSeries Navigator.
   b. Stáhněte vydavatele certifikátu (CA) ze systému, ve kterém byl vytvořen.

**Poznámka:** Vybere-li si Tom certifikát od vydavatele certifikátu (CA), jehož certifikát není v databázi klíčů jeho klienta iSeries Access for Windows, musí přidat certifikát do databáze, aby mohl používat SSL.

**Kroky při konfiguraci**

Dříve, než může Tom aktivovat SSL v produktu Centrální správa, musí nainstalovat nezbytné programy a nastavit digitální certifikáty na serveru iSeries. (Dříve, než budete pokračovat, prostudujte si část Nezbytné předpoklady). Jakmile Tom splní všechny nezbytné předpoklady, může dokončit následující proceduru a aktivovat SSL pro produkt Centrální správa.

**Poznámka:** Je-li aktivován SSL pro produkt iSeries Navigator, Tom ho musí nejdříve deaktivovat, aby mohl aktivovat SSL pro produkt Centrální správa. Jestliže je SSL aktivován pro produkt iSeries Navigator, a nikoli pro produkt Centrální správa, pokusy produktu iSeries Navigator o spojení s centrálním systémem Centrální správy selžou.

**Autentizace serveru zahrnuje tyto kroky (povinné):**

1. Konfigurace centrálního systému pro autentizaci serveru.
2. Konfigurace koncových systémů pro autentizaci serveru.

**Autentizace klienta zahrnuje tyto kroky (volitelné):**

**Poznámka:** Konfigurace autentizace klienta nemůže být dokončena, dokud není nakonfigurována autentizace serveru.

1. Konfigurace centrálního systému pro autentizaci klienta.
2. Konfigurace koncových systémů pro autentizaci klienta.

**Konfigurování centrálního systému pro autentizaci serveru**

SSL umožní Tomovi zabezpečit ochranu přenosů mezi centrálním systémem a koncovým systémem i mezi klientem produktu iSeries Navigator a centrálním systémem. SSL umožňuje přenos a autentizaci certifikátů a kódování dat. Spojení SSL může nastat pouze mezi centrálním systémem podporujícím SSL a koncovým systémem podporujícím SSL. Tom musí před autentizací klienta nastavit autentizaci serveru.

1. V prostředí produktu iSeries Navigator klepněte pravým tlačítkem myši na volbu **Centrální správa** a vyberte **Vlastnosti**.
2. Klepněte myší na ouško **Zabezpečení** a vyberte **Použít SSL (Secure Sockets Layer).**
3. Pro úroveň aktualizace vyberte volbu **Server**.
4. Klepněte myší na **OK** a nastavte tuto hodnotu v centrálním systému.

   **Poznámka:** **Nespouštějte** znovu server Centrální správy, dokud není provedena konfigurace koncových systémů pro autentizaci serveru.
5. Konfigurace koncových systémů pro autentizaci serveru.

**Konfigurace koncových systémů pro autentizaci serveru**

Jakmile Tom aktivoval SSL v centrálním systému pro autentizaci serveru, musí aktivovat SSL pro všechny koncové systémy pro autentizaci serveru. Při konfiguraci koncových systémů tak, aby mohly používat SSL, a při autentizaci serveru, postupujte takto:

1. Rozbalte okno **Centrální správa**.
2. **Porovnejte a aktualizujte systémové hodnoty pro koncové systémy:**
   a. Pod **Koncové systémy** klepněte pravým tlačítkem myši na centrální systém a vyberte **Soupis—>Shromažďování**.
   b. V dialogu Shromažďování zaškrtněte volbu **Systémové hodnoty**, abyste shromáždili soupis systémových hodnot pro centrální systém. Zrušte všechny ostatní volby.
   c. Klepněte pravým tlačítkem myši na **Skupiny systémů—>Nová skupina systémů**.
   d. Definujte novou skupinu systémů, která zahrnuje všechny koncové systémy, ke kterým se připojujete přes SSL.
   e. Jestliže chcete zobrazit novou skupinu, rozbalte seznam skupin systémů.

f. Jakmile skončíte s výběrem, klepněte pravým tlačítkem myši na novou skupinu systémů a vyberte **Systémové hodnoty —>Porovnání a aktualizace**.
g. Ověřte, že se centrální systém zobrazí v poli **Modelový systém**.
h. Vyberte kategorii **Centrální správa** a ověřte tyto hodnoty (přitom zaškrtněte vedlejší políčko):
   - Použít SSL (Secure Sockets Layer) je nastaveno na **Ano**.
   - Úroveň autentizace přes SSL je nastavena na **Server** .

   Tyto hodnoty jsou nastaveny v centrálním systému během procedury Konfigurace centrálního systému pro autentizaci serveru.
i. Klepněte myší na **OK** a nastavte tyto hodnoty v koncových systémech v nové skupině systémů.
j. Počkejte, než se ukončí proces **Porovnání a aktualizace**, a potom znovu spusťte server Centrální správy. To může trvat několik minut.

3. **Opakované spuštění serveru Centrální správy v centrálním systému:**
   a. V prostředí produktu iSeries Navigator rozbalte **Připojení**.
   b. Rozbalte okno centrálního systému.
   c. Rozbalte **Síť—> Servery** a vyberte **TCP/IP**.
   d. Klepněte pravým tlačítkem myši na volbu **Centrální správa** a vyberte **Zastavit**. Okno centrálního systému se zavře a zobrazí se zpráva, že již nejste připojeni k serveru.
   e. Jakmile se server Centrální správy zastaví, klepněte myší na **Spustit** a server znovu spusťte.
4. **Opakované spuštění serveru Centrální správy ve všech koncových systémech:**
   a. Rozbalte koncový systém, který znovu spouštíte.
   b. Rozbalte **Síť—> Servery** a vyberte **TCP/IP**.
   c. Klepněte pravým tlačítkem myši na volbu **Centrální správa** a vyberte **Zastavit**.
   d. Jakmile se server Centrální správy zastaví, klepněte myší na **Spustit** a znovu ho spusťte.
   e. Opakujte tuto proceduru pro všechny koncové systémy.
5. **Aktivace SSL pro klienta produktu iSeries Navigator:**
   a. V prostředí produktu iSeries Navigator rozbalte **Připojení**.
   b. Klepněte pravým tlačítkem myši na centrální systém a vyberte **Vlastnosti**.
   c. Klepněte myší na ouško **Secure Sockets** a vyberte **Použít SSL (Secure Sockets Layer) pro připojení**.
   d. Ukončete produkt iSeries Navigator a znovu ho spusťte.

Když Tom nyní dokončil konfiguraci autentizace serveru, může provést tyto volitelné procedury autentizace klienta:

- Konfigurace centrálního systému pro autentizaci klienta.
- Konfigurace koncových systémů pro autentizaci klienta.

Autentizace klienta umožňuje ověřit platnost vydavatele certifikátu (CA) a důvěryhodné skupiny pro koncové systémy i pro centrální systém.

### Konfigurace centrálního systému pro autentizaci klienta

Když se centrální systém (klient SSL) pokouší použít iSeries SSL k připojení ke koncovému systému (server SSL), centrální systém a koncový systém si navzájem autentizují certifikáty prostřednictvím autentizace klienta (v produktu Centrální správa se to nazývá Vydavatel certifikátu (CA) a Důvěryhodná skupina).

1. V prostředí produktu iSeries Navigator klepněte pravým tlačítkem myši na volbu **Centrální správa** a vyberte **Vlastnosti**.
2. Klepněte na ouško **Zabezpečení** a vyberte **Použít SSL (Secure Sockets Layer)**.
3. Pro úroveň autentizace vyberte volbu **Klient a server**.

4. Klepněte myší na **OK** a nastavte tuto hodnotu v centrálním systému.

   **Poznámka:** **Nespouštějte** znovu server Centrální správy, dokud nejsou všechny koncové systémy nakonfigurovány pro použití iSeries SSL při autentizaci serveru a klienta.

5. Nakonfigurujte koncové systémy pro autentizaci klienta.

**Konfigurace koncových systémů pro autentizaci klienta**

1. **Porovnání a aktualizace systémových hodnot pro koncové systémy:**

   **Poznámka:** Tato úloha nefunguje pro všechny koncové servery iSeries, na nichž je provozována verze V4R5. Viz červená kniha verze V4R4 ″Management Central: A Smart Way to Manage AS/400 Systems″.

   a. Pod **Koncové systémy** klepněte pravým tlačítkem myši na centrální systém a vyberte **Soupis—>Shromažďování**.
   b. V dialogu Shromažďování zaškrtněte volbu **Systémové hodnoty**, abyste shromáždili soupis systémových hodnot pro centrální systém. Zrušte všechny ostatní volby.
   c. Klepněte pravým tlačítkem myši na **Skupiny systémů—>Nová skupina systémů**.
   d. Definujte novou skupinu systémů, která zahrnuje všechny koncové systémy, ke kterým se připojujete pomocí SSL.
   e. Jestliže chcete zobrazit novou skupinu, rozbalte seznam skupin systémů.
   f. Jakmile skončíte s výběrem, klepněte pravým tlačítkem myši na novou skupinu systémů a vyberte **Systémové hodnoty —>Porovnání a aktualizace**.
   g. Ověřte, že se centrální systém zobrazí v poli **Modelový systém**.
   h. Vyberte kategorii **Centrální správa** a ověřte toto:
      - Použít SSL (Secure Sockets Layer) je nastaveno na **Ano**.
      - Úroveň autentizace přes SSL je nastavena na **Klient a server**.

      Tyto hodnoty jsou nastaveny v centrálním systému během procedury Konfigurace centrálního systému pro autentizaci klienta. Zaškrtněte políčko **Aktualizace** vedle každé hodnoty.
   i. Klepněte myší na **OK** a nastavte tyto hodnoty v koncových systémech v nové skupině systémů.

2. **Kopírování ověřovacího seznamu do koncových systémů:**
   a. V prostředí produktu iSeries Navigator rozbalte **Centrální správa—>Definice**.
   b. Klepněte pravým tlačítkem myši na **Sada programů** a vyberte **Nová definice**.
   c. V okně **Nová definice** pracujte s těmito volbami:
      - **Jméno:** Napište jméno definice.
      - **Zdrojový systém:** Vyberte jméno centrálního systému.
      - **Vybrané soubory a pořadače:** Klepněte myší na pole a napište /QSYS.LIB/QUSRSYS.LIB/QYPSVLDL.VLDL.
   d. Klepněte myší na ouško **Volby** a vyberte **Nahradit existující soubor odesílaným souborem**.
   e. Klepněte myší na **Rozšířené**.
   f. V okně **Rozšířené volby** zadejte **Ano**, čímž povolíte rozdíly objektů při obnově.
   g. Klepněte myší na **OK**, čímž obnovíte seznam definic a zobrazíte novou sadu.
   h. Klepněte pravým tlačítkem myši na novou sadu a vyberte **Odeslat**.
   i. V dialogu ″**Odeslat**: Přidat důvěryhodnou skupinu″ odstraňte všechny ostatní volby a klepněte myší na **OK**. Důvěryhodná skupina je skupinou systémů, kterou jste definovali v kroku 1 této procedury.

**Poznámka:** Úloha **Odeslat** v centrálním systému vždycky selže, protože centrální systém je vždy zdrojovým systémem. Úloha **Odeslat** by se měla úspěšně provést ve všech koncových systémech.

3. **Opětovné spuštění serveru Centrální správy v centrálním systému:**
   a. V prostředí produktu iSeries Navigator rozbalte **Připojení**.
   b. Rozbalte centrální systém.
   c. Rozbalte **Síť—> Servery** a vyberte **TCP/IP**.
   d. Klepněte pravým tlačítkem myši na volbu **Centrální správa** a vyberte **Zastavit**. Okno centrálního systému se zavře a zobrazí se zpráva, že již nejste připojeni k serveru.
   e. Jakmile se server Centrální správy zastaví, klepněte myší na **Spustit** a server znovu spusťte.
4. **Opakované spuštění serveru Centrální správy ve všech koncových systémech:**

   **Poznámka:** Opakujte tuto proceduru pro všechny koncové systémy.
   a. Rozbalte znovu spouštěný koncový systém.
   b. Rozbalte **Síť—> Servery** a vyberte **TCP/IP**.
   c. Klepněte pravým tlačítkem myši na volbu **Centrální správa** a vyberte **Zastavit**.
   d. Jakmile se server Centrální správy zastaví, klepněte myší na **Spustit** a server znovu spusťte.

# Kapitola 4. Koncepce SSL

S protokolem SSL můžete mezi klientskými a serverovými aplikacemi vytvořit bezpečné spojení, které umožní autentizaci jednoho nebo obou koncových bodů komunikační relace. Protokol SSL také poskytuje soukromí a integritu dat vyměňovaných mezi klientskými a serverovými aplikacemi.

Následující informace vám pomohou lépe pochopit vztah mezi SSL a serverem iSeries:

- Historie SSL.
- Jak SSL pracuje.
- Podporované protokoly SSL a TLS (Transport Layer Security).
- Autentizace serveru.
- Autentizace klienta.

## Historie SSL

Protokol SSL (Secure Sockets Layer) vyvinula společnost Netscape v roce 1994 jako odpověď na rostoucí zájem o bezpečnost v síti Internet. Přestože byl protokol SSL původně vyvinut pro zabezpečení komunikace mezi prohlížeči WWW a servery, jeho specifikace byla navržena takovým způsobem, že jiné aplikace, jako je TELNET a FTP, ho mohou používat také. Více informací o SSL a souvisejících protokolech najdete v části Podporované protokoly SSL and TLS (Transport Layer Security).



## Jak SSL pracuje

SSL jsou vlastně dva protokoly. Je to záznamový protokol a protokol pro navazování spojení. Záznamový protokol řídí tok dat mezi dvěma koncovými body relace SSL.

Protokol pro navazování spojení autentizuje jeden nebo oba koncové body relace SSL a vytváří jedinečný symetrický klíč pro generování klíčů sloužících ke kódování a dekódování dat pro relaci SSL. SSL používá asymetrické šifrování, digitální certifikáty a toky navazování spojení SSL k autentizaci jednoho nebo obou koncových bodů relace SSL. Obvykle je autentizován server a volitelně také klient. Digitální certifikát vydaný vydavatelem certifikátu (CA) může být přiřazen každému koncovému bodu nebo aplikacím používajícím SSL na každém koncovém bodu spojení.

Digitální certifikát obsahuje veřejný klíč a některé identifikační informace, které byly digitálně podepsány důvěryhodným vydavatelem certifikátu (CA). Každý veřejný klíč má asociovaný privátní klíč. Privátní klíč není uložen s certifikátem ani není jeho součástí. Při autentizaci serveru i klienta musí autentizovaný koncový bod prokázat, že má přístup k privátnímu klíči asociovanému s veřejným klíčem v digitálním certifikátu.

Navazování spojení SSL je časově náročná operace v důsledku šifrovacích operací pomocí veřejných a privátních klíčů. Po vytvoření počáteční relace SSL mezi dvěma koncovými body může být informace o relaci SSL pro tyto dva koncové body a aplikace uložena do bezpečné paměti kvůli urychlení aktivace následné relace SSL. Když relace SSL pokračuje, oba koncové body použijí zkrácený tok navazování spojení k autentizaci toho, zda má každý z nich přístup k jedinečným informacím bez použití veřejného nebo privátního klíče. Jestliže oba koncové body mohou prokázat, že mají přístup k těmto jedinečným informacím, vytvoří se nové symetrické klíče a relace SSL ″pokračuje″. U relací TLS verze 1.0 a SSL verze 3.0 nezůstane uložená informace v bezpečné paměti déle než 24 hodin. Ve verzi V5R2M0 může být vliv navazování spojení SSL na výkon hlavního CPU minimalizován pomocí šifrovacího hardwaru.

## Podporované protokoly SSL and TLS

Existuje několik definovaných verzí protokolu SSL. Nejnovější verze TLS (Transport Layer Security) je založena na SSL 3.0 a je produktem společnosti IETF (Internet Engineering Task Force). Implementace OS/400 podporuje tyto verze protokolů SSL a TLS:

- TLS verze 1.0
- TLS verze 1.0 s kompatibilitou SSL verze 3.0

  **Poznámky:**

  1. Specifikace TLS verze 1.0 s kompatibilitou SSL verze 3.0 znamená, že o protokolu TLS se bude vyjednávat, zda je možný, a když možný nebude, bude se vyjednávat o protokolu SSL verze 3.0. Jestliže není možné vyjednávat o protokolu SSL verze 3.0, navazování spojení SSL selže.
  2. Podporujeme také TLS verze 1.0 s kompatibilitou SSL verze 3.0 a SSL verze 2.0. To je specifikováno hodnotou protokolu **ALL**, což znamená, že o protokolu TLS se bude vyjednávat, zda je možný, a když možný nebude, bude se vyjednávat o protokolu SSL verze 3.0. Jestliže není možné vyjednávat o protokolu SSL verze 3.0, bude se vyjednávat o protokolu SSL verze 2.0. Jestliže není možné vyjednávat o protokolu SSL verze 2.0, navazování spojení SSL selže.
- SSL verze 3.0
- SSL verze 2.0
- SSL verze 3.0 s kompatibilitou SSL verze 2.0

### SSL verze 3.0 versus SSL verze 2.0

Protokol SSL verze 3.0 je ve srovnání s protokolem SSL verze 2.0 téměř úplně jiným protokolem. Některé z hlavních rozdílů mezi oběma protokoly zahrnují tyto odlišnosti:

- Protokoly pro navazování spojení SSL verse 3.0 jsou jiné, než protokoly pro navazování spojení SSL verze 2.0.
- SSL verze 3.0 používá implementaci BSAFE 3.0 od společnosti RSA Data Security, Inc. BSAFE 3.0 zahrnuje řadu oprav útoků souvisejících s časováním a SHA-1 algoritmus přepočtu klíče. The SHA-1 algoritmus přepočtu klíče je pokládán za bezpečnější, než MD5 algoritmus přepočtu klíče. SHA-1 umožňuje protokolu SSL verze 3.0 podporovat další šifrovací sady, které používají SHA-1 namísto MD5.
- Protokol SSL verze 3.0 potlačuje výskyt útoků typu MITM (man-in-the-middle) během zpracování navazování spojení SSL. V protokolu SSL verze 2.0 bylo možné, i když nepravděpodobné, aby útok MITM oslabil specifikaci šifrování. Oslabení šifrování by mohlo umožnit neoprávněné osobě odhalit klíč relace SSL.

### TLS verze 1.0 versus SSL verze 3.0

TLS (Transport Layer Security) verze 1.0 je založen na SSL verze 3.0 a je nejnovějším protokolem SSL, který je odvětvovým standardem. Jeho specifikace jsou definovány společností IETF (Internet Engineering Task Force) ve verzi RFC 2246 v části ″The TLS Protocol″. 

Hlavním cílem TLS je učinit SSL bezpečnější a současně učinit protokol přesnější a dokonalejší. TLS umožňuje tato zlepšení SSL verze 3:

- Bezpečnější algoritmus MAC.
- Přesnější výstrahy.
- Jasnější definici specifikací ″šedé oblasti″.

Všechny aplikace serveru iSeries, které jsou aktivovány pro SSL, získají automaticky podporu TTL. Výjimkou jsou případy, kdy aplikace výslovně žádala o použití pouze SSL verze 3.0 nebo SSL verze 2.0.

TLS poskytuje tato zlepšení zabezpečení ochrany dat:

- **Kód HMAC (Key-Hashing for Message Authentication)**
  TLS používá kód HMAC (Key-Hashing for Message Authentication Code), který zajišťuje, že záznam nemůže být změněn během cesty v nechráněné síti, jako je Internet. SSL verze 3.0 umožňuje také autentizaci klíčované zprávy, ale kód HMAC je pokládán za bezpečnější, než funkce MAC (Message Authentication Code), kterou používá SSL verze 3.0.
- **Funkce PRF (Enhanced Pseudorandom Function)**
  Funkce PRF se používá pro generování dat klíče. V TLS je funkce PRF definována pomocí kódu HMAC. Funkce PRF používá dva algoritmy pro přepočet klíče takovým způsobem, který zaručuje její bezpečnost. Pokud je jeden z algoritmů odkrytý, potom data zůstanou bezpečná, když zůstane druhý algoritmus chráněný.
- **Zdokonalené ověřování zprávy o dokončení**
  Jak TLS verze 1.0, tak SSL verze 3.0 poskytuje zprávu o dokončení pro oba koncové body, která autentizuje, že vyměněné zprávy nebyly změněny. TLS však odvozuje tuto zprávu o ukončení od hodnot PRF a HMAC, což je opět bezpečnější, než SSL verze 3.0.
- **Konzistentní zpracování certifikátů**
  Na rozdíl od SSL verze 3.0 se TLS pokouší určit typ certifikátu, který si musí vyměnit implementace TLS.
- **Specifické varovné zprávy**
  TLS poskytuje konkrétnější a nové varovné zprávy pro označení problémů, které některý z koncových bodů relace detekuje. TLS také dokumentuje, kdy by měly být odeslány určité varovné zprávy.

## Autentizace serveru

Při autentizaci serveru klient zajistí, že je platný certifikát serveru a že je tento certifikát podepsaný vydavatelem certifikátu (CA), kterému klient důvěřuje. SSL použije asymetrické šifrování a protokoly pro navazování spojení pro generování symetrického klíče, který se použije pouze pro tuto jedinečnou relaci SSL. Tento klíč se použije pro generování sady klíčů, jenž se použijí pro kódování a dekódování dat, která tečou v relaci SSL. Po dokončení navazování spojení SSL se autentizuje jeden nebo oba konce komunikační linky a vygeneruje se jedinečný klíč pro kódování a dekódování dat. Jakmile je ukončeno navazování spojení, tečou zakódovaná data aplikační vrstvy v relaci SSL.

## Autentizace klienta

Mnoho aplikací umožňuje aktivovat autentizaci klienta. Při autentizaci klienta server zajistí, že je platný certifikát klienta a že je tento certifikát podepsaný vydavatelem certifikátu (CA), kterému server důvěřuje. Následující aplikace serveru iSeries podporují autentizaci klienta:

- Server IBM HTTP Server.
- Server IBM HTTP Server (provozovaný na bázi Apache).
- Server FTP.
- Server Telnet.
- Koncový systém Centrální správy.
- LDAP (Directory Services).

# Kapitola 5. Plánování umožnění SSL

Když plánujete umožnění SSL na serveru iSeries, musíte vzít v úvahu níže uvedené skutečnosti:

- Nezbytné předpoklady pro SSL.
- Jaký typ digitálních certifikátů chcete a kde je získáte.

**Nezbytné předpoklady pro SSL**:

- Produkt IBM DCM (Digital Certificate Manager), volba 34 operačního systému OS/400 (5722-SS1).
- TCP/IP Connectivity Utilities for iSeries (5722-TC1).
- IBM HTTP Server for iSeries (5722-DG1).
- Jestliže se pokoušíte použít server HTTP Server, abyste mohli použít produkt DCM, ujistěte se, že máte nainstalován produkt IBM Developer Kit for Java (5722–JV1), jinak se server HTTP Administration Server nespustí.
- Produkt IBM Cryptographic Access Provider, 5722-AC3 (128bitový). Počet bitů pro tento produkt označuje maximální velikost utajovaného materiálu v symetrických klíčích, který může být použit v šifrovacích operacích. Velikost povolená pro symetrický klíč se řídí exportními a importními zákony každé země. Vyšší počet bitů má za následek bezpečnější spojení.
- Můžete také instalovat šifrovací hardware pro použití se SSL, abyste urychlili navazování spojení SSL. Od verze V5R2M0 máte k dispozici tyto šifrovací hardwarové volby pro použití se serverem iSeries:
  - 2058 Cryptographic Accelerator (kód hardwarové komponenty 4805).
  - 4758 Cryptographic Coprocessor (kódy hardwarové komponenty 4801 nebo 4802).

  Chcete-li instalovat šifrovací hardware, musíte nainstalovat také volbu 35 Cryptographic Service Provider.

Jestliže chcete používat SSL s některou komponentou produktu iSeries Access for Windows nebo IBM Toolbox for Java, musíte nainstalovat také produkt iSeries Client Encryption, 5722-CE3 (128bitový). Produkt iSeries Access for Windows potřebuje tento produkt, aby vytvořil bezpečné spojení.

**Poznámka:** Nemusíte instalovat Client Encryption Product, abyste mohli používat emulátor PC5250, který se dodává s produktem Personal Communications. Produkt Personal Communications má svůj vestavěný šifrovací kód.

**Digitální certifikáty**

Přečtěte si téma Použití veřejných certifikátů versus použití privátních certifikátů, abyste lépe pochopili rozdíly mezi veřejnými a privátními digitálními certifikáty a dověděli se o možnostech jejich získání.

Produkt IBM DCM (Digital Certificate Manager) je řešení serveru iSeries pro správu digitálních certifikátů. Více informací o produktu DCM najdete v rámci aplikace Information Center pod tématem Digital Certificate Manager.

# Kapitola 6. Zabezpečení aplikací pomocí SSL

Pomocí SSL můžete zabezpečit ochranu těchto aplikací serveru iSeries:

- IBM HTTP Server for iSeries.
- IBM HTTP Server for iSeries (provozovaný na bázi Apache).
- Server FTP.
- Server Telnet.
- Server DRDA (distributed relational database architecture) a DDM (distributed data management).
- Centrální správa.
- LDAP (Directory Services Server)
- EIM (Enterprise Identity Mapping)
- Aplikace iSeries Access for Windows včetně produktu iSeries Navigator.
- Aplikace, které jsou zapsány do sady rozhraní API produktu iSeries Access for Windows.
- Programy vyvinuté pomocí produktu Developer Kit for Java a klientské aplikace, které používají IBM Toolbox for Java.
- Aplikace vyvinuté pomocí rozhraní Secure Sockets API podporovaných na serveru iSeries. Podporovaná rozhraní API jsou GSKit (Global Secure Toolkit) a nativní rozhraní API SSL_ iSeries. Informace o GSKit a SSL_API najdete pod tématem Secure Sockets APIs.

# Kapitola 7. Odstraňování problémů se SSL

Tyto základní informace o odstraňování problémů vám mají pomoci zredukovat seznam možných problémů, které může server iSeries detekovat u SSL. Je důležité, abyste pochopili, že toto není vyčerpávající zdroj informací pro odstraňování problémů, ale pouze průvodce.

Ověřte, že jsou pravdivá tato tvrzení:

- Splnili jste nezbytné předpoklady pro SSL na serveru iSeries (viz část Nezbytné předpoklady pro SSL).
- Používáte-li komponentu Centrální správa produktu iSeries Navigator se systémem V5R1, nainstalovali jste v systému tato PTF:
  - si01375
  - si01376
  - si01377
  - si01378
  - si01838
- Váš vydavatel certifikátu (CA) a certifikáty jsou platné a nemají prošlé datum.

Jestliže jste ověřili, že předcházející tvrzení jsou pravdivá, a stále máte na serveru iSeries problém související se SSL, můžete zkusit tyto volby:

- Chybový kód SSL v protokolu úloh serveru může mít křížovou referenci v tabulce chyb, kde můžete najít více informací o chybě. Informace o chybových zprávách rozhraní Secure Sockets API najdete na stránce Chybové zprávy o kódech rozhraní Secure Sockets API. Například tato tabulka mapuje -93, které se mohou objevit v protokolu úloh serveru pro konstantu SSL_ERROR_SSL_NOT_AVAILABLE .
  - Negativní návratový kód (určený pomlčkou před číslem kódu) označuje, že používáte SSL_ API.
  - Pozitivní návratový kód označuje, že používáte GSKit API. Programátoři mohou naprogramovat gsk_strerror() nebo SSL_Strerror() API v programech, aby získali stručný popis návratového kódu chyby. Některé aplikace využijí tato rozhraní API a vytisknou zprávu do protokolu úloh, která obsahuje tuto větu.

  Pokud požadujete podrobnější informace, je možné na serveru iSeries zobrazit ID zprávy uvedené v tabulce kvůli zjištění možné příčiny chyby a možnosti jejího odstranění. Další dokumentaci vysvětlující tyto chybové kódy je možné najít v jednotlivých rozhraních Secure Sockets API, která vrátila chybu.
- Níže uvedené soubory záhlaví obsahují stejná jména konstant pro návratové kódy systémového SSL jako tabulka, ale bez křížové reference ID zprávy:
  - QSYSINC/H.GSKSSL
  - QSYSINC/H.SSL

  Pamatujte si, že přestože jména návratových kódu systémového SSL zůstávají v těchto dvou souborech konstantní, s každým návratovým kódem může být asociována více než jedna jedinečná chyba.

Více informací týkajících se serveru iSeries najdete pod tématem Troubleshooting and service.

# Kapitola 8. Související informace

Další informace o SSL můžete najít v těchto zdrojích:

**Zdroje IBM**

- Stránka SSL and Java Secure Socket Extension (JSSE) obsahuje stručný popis JSSE a jejího použití.
- Stránka Java Secure Socket Layer (JSSL) obsahuje stručný popis JSSL a jejího použití.
- Stránka IBM Toolbox for Java obsahuje stručný popis dostupných tříd Java a jejich použití.

**RFC (Request for Comments)**

- RFC 2246: ″The TLS Protocol Version 1.0 ″ vysvětluje podrobně protokol TLS.
- RFC2818: ″HTTP Over TLS″ popisuje, jak použít TLS pro zabezpečení připojení HTTP na Internetu.

**Jiné zdroje**

- Dokument The SSL Protocol Version 3.0 vysvětluje podrobně protokol SSL verze 3.0.

Vytištěno v  Dánsku společností IBM Danmark A/S.