

## 4 Technická specifikace dodávky (navrhované technické řešení)

### 1.1 Přípravná fáze implementace

Cílem přípravné fáze implementace je:

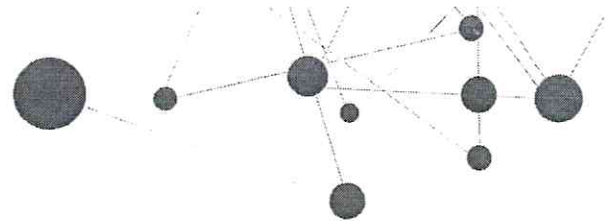
1. Sestavení projektového týmu
  - a. Zadavatel
    - i. Projektový vedoucí
    - ii. Metodik (finanční řízení)
    - iii. Správce řešení (uživatelský)
    - iv. Správce řešení (technický)
  - b. Realizátor
    - i. Metodik (finanční řízení)
    - ii. Vedoucí implementátor
    - iii. Projektový vedoucí (může být dosazená stejná osoba jako vedoucí implementátor)
2. Příprava produkčních, verifikačních a školicích prostředí.
3. Zajištění přístupů k jednotlivým prostředím a komponentám nutných pro správu řešení
4. Zajištění spolupráce 3. stran
5. Aktualizace a předání technické a uživatelské dokumentace.
6. Proškolení administrátorů a technických správců zadavatele v nastavených procesech na pilotní implementaci (verifikační prostředí u zadavatele).
7. Proškolení hlavních uživatelů zadavatele v užívání a správě řešení na pilotní implementaci (verifikační prostředí u zadavatele).

### 1.2 Dodávka a implementace softwarového nástroje pro oblast Finančního řízení

DYNATECH poskytuje nabyvateli nevýhradní, nepřenosné, časově, množstevně a teritoriálně neomezené právo užívat software CROSEUS, který je určen pro podporu procesu finanční kontroly (modul CROSEUS-Finanční kontrola), finančního plánování (modul CROSEUS-Finanční plán), monitorování (modul CROSEUS-Continuous Monitoring) a dále modul Registr smluv. Licence se poskytuje jako multilicence, u které není rozhodující počet uživatelů a to po celou dobu trvání smluvního vztahu.

Součástí dodávky je také poskytnutí CROSEUS API integračního rozhraní včetně realizace integrace na stávající ekonomický systém zadavatele, FEIS od společnosti ARBES a licence pokrývající úpravy FIES pro nastavení integrace včetně implementace úprav FEIS.

Subdodavatelem úprav IS FEIS je firma ARBES Technologies s.r.o. Náklady spojené s úpravou IS FEIS hradí dodavatel. Mezi firmou DYNATECH s.r.o. a firmou ARBES Technologies s.r.o. byla uzavřena smlouva o subdodávce úprav IS FEIS.



### Finanční plán

Modul umožňuje sestavení, realizaci a sledování finančního plánu Příspěvkové organizace. Finanční plán je možné sestavit dle 30 uživatelsky nastavitelných dimenzí, pro které je možné plánovat a sledovat tok finančních prostředků. Jeho realizace se děje automaticky při schvalování jednotlivých účetních dokladů v rámci modulu Finanční kontrola.

### Finanční kontrola

Modul slouží pro schvalování průvodních dokladů k objednávkám, smlouvám, fakturám, platebním poukazům atp. Modul umožňuje zaznamenání provedení nejen předběžné finanční kontroly před a po vzniku závazku, ale i vykonání průběžné a následné finanční kontroly k jednotlivým operacím. Výsledkem schvalování je doklad o provedení finanční kontroly a detailní auditní stopa, která obsahuje úplnou časovou posloupnost provedených kroků a všechny příslušné dokumenty formou přílohy.

CROSEUS Finanční kontrola obsahuje tyto základní kontrolní mechanismy

- Soulad časového období.
- Soulad chronologie řídicí kontroly.
- Soulad finanční výše
- Soulad subjektů
- Soulad finančního krytí
- Shoda položek věcného plnění, finančního krytí a předkontace s celkovou částkou.
- Kontrola obsazení rolí s právem rozhodnutí.
- Kontrola připojení dokladu po vzniku závazku/nároku k dokladu před vznikem závazku/nároku.
- Kontrola spolehlivosti plátce DPH a zveřejnění účtu.

### Registr smluv

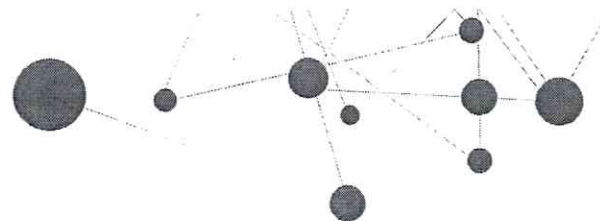
Pomocí modulu Registr smluv můžete přímo po schvalovacím procesu, uveřejnit závazek do registru smluv. Automaticky probíhají nad tímto krokem kontrolní mechanismy, které jsou nastaveny dle zákona č. 340/2015 Sb. (např. čitelnost smlouvy; vyplnění povinných údajů smlouvy atd.)

### Manažerský informační systém

Manažerský informační systém bude dodán jako sada reportů v technologii MS SQL společně s jednou licencí na nastavbu v prostředí Power BI.

### Ekonomická hlediska:

- Celkový objem schvalovaných finančních prostředků za vybrané období a pro vybrané středisko



- Nejvyšší schvalovaná částka
- Průměrná schvalovaná částka
- Celková finanční výše závazků a výdajů dle subjektů/středisek/komodit.

#### Výkonnostní ukazatele:

- Celkový počet schválených dokladů za vybrané období/středisko/komoditu
- Počet nově založených dokladů za vybrané období.
- Průměrná délka schvalování vybraného typu dokladu za vybrané období/středisko

#### Ukazatele

- Rizika
  - Subjekty – nespolehlivost plátce DPH a zveřejnění jeho účtů
  - Nedodržení data splatnosti faktur
  - Nepřipojení výdaje k závazku = nemožnost vyhodnocení neshod
- Neshody u operací
  - Rozdílnost subjektů
  - Chronologie právní a finanční fáze
  - Finanční výše
  - Finančního krytí
  - Časového období u limitovaných

Přílohou popisu produktu je Technická příručka, viz kap. 10.3.

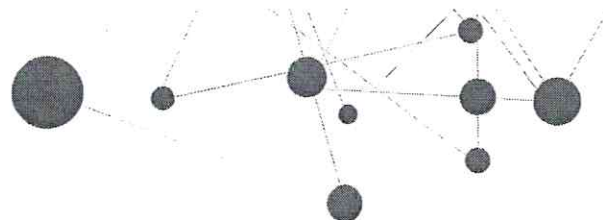
#### **1.2.1 Analýza a optimalizace procesů**

1. Analýza procesů finanční kontroly a finančního plánování (nutná součinnost zodpovědných osob).
2. Optimalizace procesů tak aby mohli být elektronizovány
  - a. Metodické nastavení (směrnice) v oblasti výkonu finanční kontroly,
  - b. Školení v oblasti metodického nastavení procesů:
  - c. Popis konfigurace SW nástrojů (vyplnění implementačního dotazníku)
3. Vypořádání připomínek

#### **1.2.2 Instalace, konfigurace, ověření SW: CROSEUS Finanční kontrola a Finanční plán**

Implementace bude mít následující průběh:

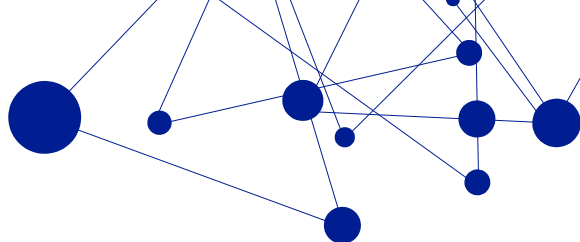
4. Konfigurace SW nástroje
  - a. Nasazení a konfigurace řešení
  - b. Příprava klientských stanic
  - c. Konfigurace integrace
  - d. Ověření konfigurace SW nástroje projektovým týmem
  - e. Vypořádání připomínek a akceptace
5. Školení uživatelů a administrátorů
  - f. Školení uživatelů
  - g. Školení klíčových uživatelů a administrátorů



6. Zkušební provoz
  - h. Současné schvalování elektronicky i papírově
  - i. Ověření integračních bodů
  - j. Vypořádání připomínek a akceptace
7. Produktivní provoz s dohledem
  - k. Produktivní nasazení
  - l. Produktivní provoz s dohledem

### 1.2.3 Instalace, konfigurace, ověření SW: CROSEUS Monitoring

8. Konfigurace SW nástroje a ověřovací provoz
  - a. Nasazení a konfigurace řešení dle „Popisu konfigurace SW nástrojů“
  - b. Příprava klientských stanic
  - c. Ověření konfigurace SW nástroje projektovým týmem
  - d. Vypořádání připomínek a akceptace
9. Školení uživatelů a administrátorů
  - e. Školení klíčových uživatelů
10. Zkušební provoz
  - f. Vytvoření 1. monitorovací zprávy
  - g. Vypořádání připomínek a akceptace
11. Produktivní provoz s dohledem
  - h. Produktivní nasazení



# CROSEUS

## TECHNICKÁ DOKUMENTACE

### DYNATECH

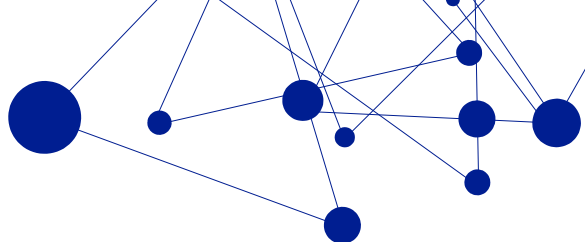
**Autor: Mgr. Radek Holčák, Marek Navrátil**

**Verze dokumentu: 1.39**

**Pro verzi aplikace: 1.32.0.19198**

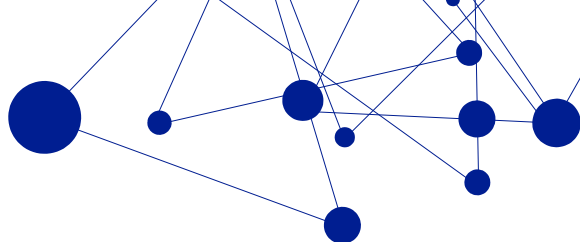
**Datum vzniku: 18.2.2013**

**Datum poslední změny: 9.11.2018**

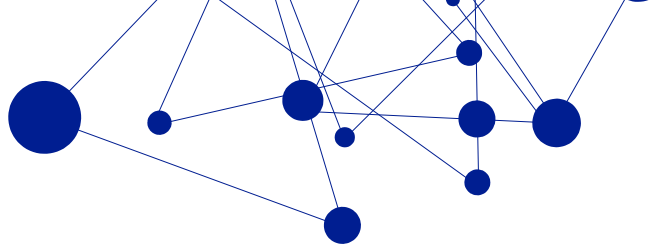


## Obsah

1	Cíl dokumentu .....	4
2	Infrastruktura systému CROSEUS .....	4
3	Komponenty systému .....	6
3.1	Aplikace CROSEUS .....	6
3.1.1	Popis .....	6
3.1.2	Konfigurace .....	8
3.1.3	Instalační postupy .....	16
3.1.4	Potřebná oprávnění .....	18
3.1.5	Minimální HW a SW nároky .....	20
3.2	Databáze CROSEUS .....	25
3.2.1	Popis .....	25
3.2.2	Konfigurace .....	25
3.2.3	Instalační postupy .....	25
3.2.4	Minimální HW a SW nároky .....	26
3.3	Aplikace Dynatech Signature Tool .....	27
3.3.1	Popis .....	27
3.3.2	Konfigurace .....	27
3.3.3	Instalační postupy .....	27
3.3.4	Potřebná oprávnění .....	30
3.3.5	Minimální HW a SW nároky .....	30
3.4	Certifikát softwarového vydavatele Dynatech .....	31
3.4.1	Popis .....	31
3.4.2	Konfigurace .....	31
3.4.3	Instalační postupy .....	31
3.4.4	Potřebná oprávnění .....	33
3.4.5	Minimální HW a SW nároky .....	33
3.5	Aplikace Dynatech Scheduler .....	34
3.5.1	Popis .....	34
3.5.2	Konfigurace .....	34
3.5.3	Instalační postupy .....	39
3.5.4	Potřebná oprávnění .....	39
3.5.5	Minimální HW a SW nároky .....	40



3.6	Integrace s CROSEUS Identity Management .....	41
3.6.1	Popis .....	41
3.6.2	Konfigurace .....	41
3.6.3	Zprovoznění integrace .....	42
3.7	Reporty CROSEUS .....	44
3.7.1	Popis .....	44
3.7.2	Konfigurace .....	45
3.7.3	Instalační postupy .....	48
3.7.4	Potřebná oprávnění .....	50
3.7.5	Minimální HW a SW nároky .....	51
3.8	Instalátor DYNATECH Installer .....	52
3.8.1	Popis .....	52
3.8.2	Konfigurace .....	52
3.8.3	Instalační postupy .....	56
3.8.4	Potřebná oprávnění .....	57
3.8.5	Minimální HW a SW nároky .....	58
4	Zálohování .....	59
4.1	Obecná doporučení pro zálohování databáze CROSEUS .....	60
4.2	Zálohování externího datového úložiště PDF dokladů .....	60
4.3	Archivace záloh .....	61
4.4	Optimalizační varianty .....	61
5	Související dokumentace .....	62



## 1 Cíl dokumentu

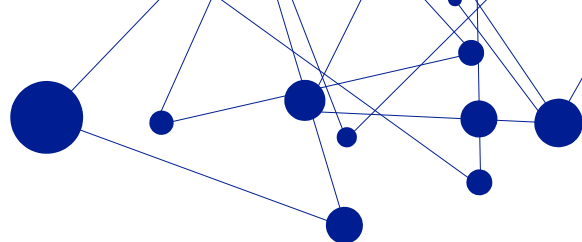
Cílem dokumentu je strukturovaně popsat komponenty systému CROSEUS firmy DYNATECH s.r.o.

## 2 Infrastruktura systému CROSEUS

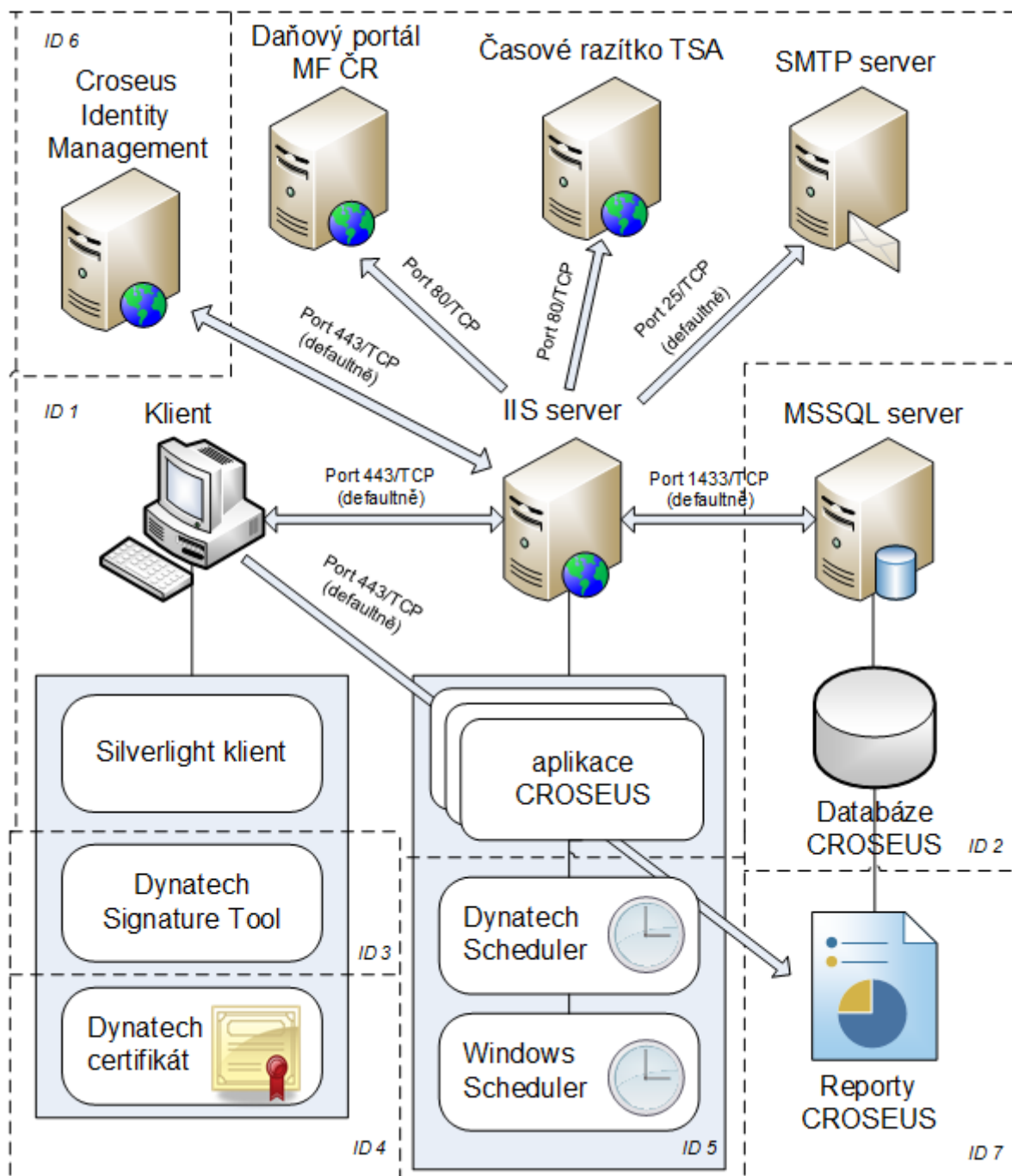
Hlavní komponenty systému CROSEUS:

1. Aplikace Dynatech CROSEUS
2. Databáze CROSEUS
3. Aplikace Dynatech Signature Tool (dále DST)
4. Certifikát vydavatele softwaru Dynatech
5. Aplikace Dynatech Scheduler
6. (volitelně) Aplikace Dynatech CROSEUS Identity Management (dále CIM)
7. (volitelně) Reporty CROSEUS
8. Instalátor Dynatech Installer

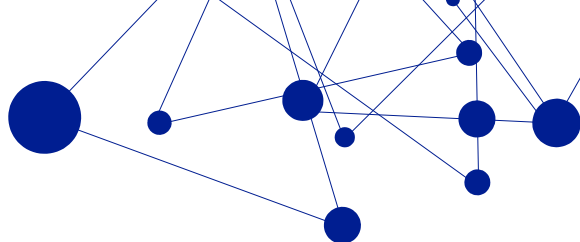




Základní komunikační schéma systému:



Detailní popis komponent, včetně přesného vymezení jejich role/vztahu k celému systému je zpracován v kapitole 3.



## 3 Komponenty systému

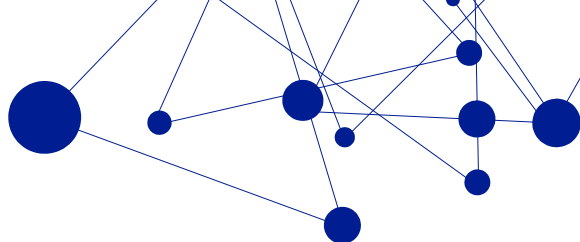
### 3.1 Aplikace CROSEUS

#### 3.1.1 Popis

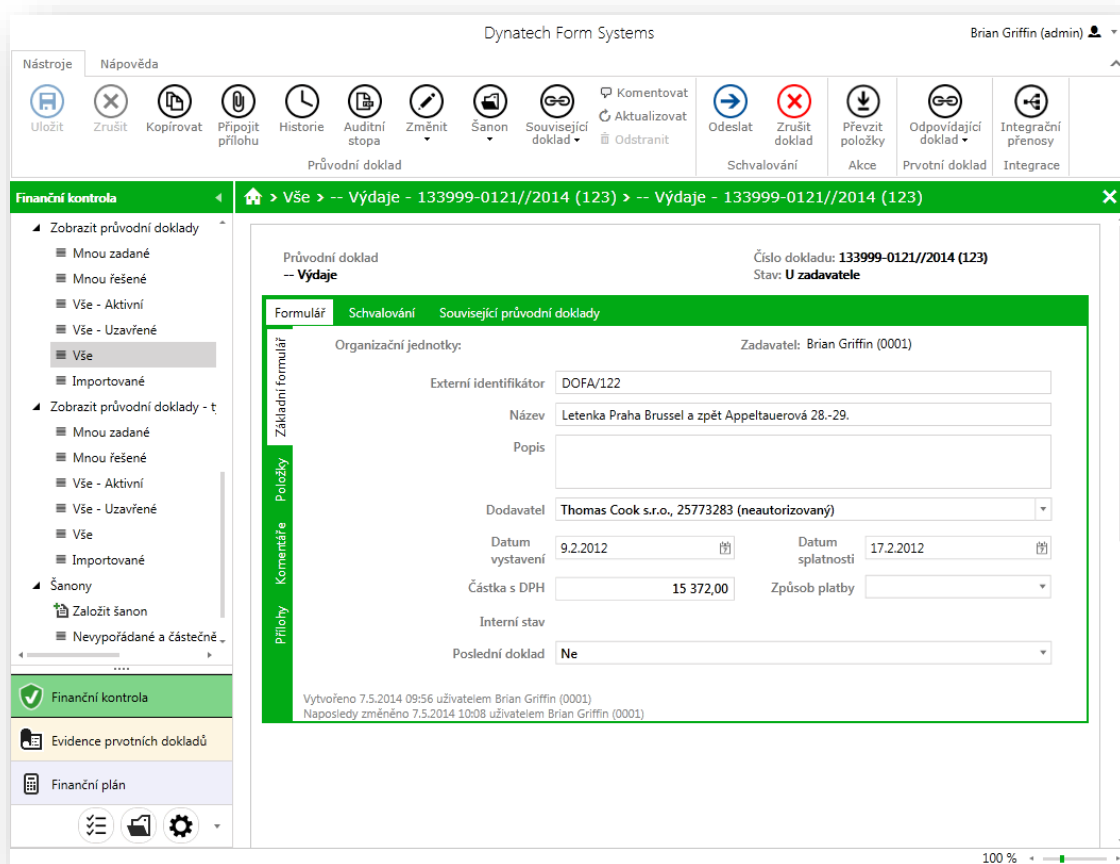
Hlavní částí aplikace CROSEUS je modul elektronické řídicí kontroly. Modul slouží pro elektronické schvalování a evidenci dokladů, které podléhají zákonu o finanční kontrole – č. 320/2001 Sb. Umožňuje uživatelům systému rozhodovat o schválení/zamítnutí či doporučení/nedoporučení jednotlivých částí operace. Celý proces schvalování je dokladován souborem typu PDF/A-3A (auditní stopa) a každý krok procesu je spojen s konkrétním uživatelem pomocí uživatelského přístupu. V systému vystupují dva typy rolí – „Role s právem doporučení“, která se vyjadřuje ve smyslu doporučuji/nedoporučuji schválení dokladu (své rozhodnutí nedokládá elektronickým podpisem) a „Role s právem rozhodnutí“, která se vyjadřuje ve smyslu schvaluji/neschvaluji (své rozhodnutí dokládá elektronickým podpisem, který může být opatřen časovým razítkem, aby byla zaručena platnost dokumentu v čase).

Aplikace je realizovaná v technologii Microsoft Silverlight. Má formu Internet Information Services (dále IIS) webu. Volitelně lze aplikaci nastavit tak, aby během procesu schvalování odesílala uživatelům informační emaily, nebo aby záznam o schválení/zamítnutí doplňovala časovým razítkem. Aplikace také sama hlídá, zda subjekty užití v procesu řídicí kontroly jsou spolehlivými plátcí DPH a umí o nich zjistit podrobnější informace na základě IČ. Ke svému běhu využívá i další komponenty, jmenovitě:

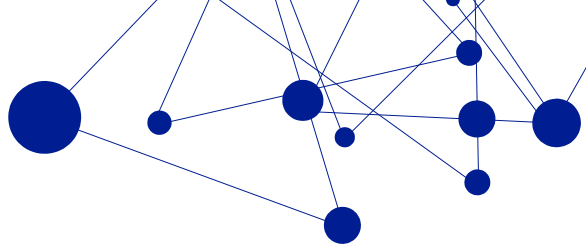
Název komponenty	Účel	Detaily	Povinná?	Určena pro
<b>databázi CROSEUS</b>	Uchovává veškerá data systému.	Oddíl 3.1.5.2	Ano	Server
<b>reporty CROSEUS</b>	Umožňují přehledně zobrazit kritické a pro management důležité vazby mezi daty z databáze CROSEUS.	Oddíl 3.7	Ne	Server
<b>aplikaci DYNATECH Signature Tools (DST)</b>	Zajišťuje elektronické podepisování výstupních dokumentů systému. Uživatel ovšem musí disponovat vhodným podpisovým certifikátem – viz níže.	Oddíl 3.3	Ne	Klientskou stanicí
<b>aplikaci DYNATECH Scheduler</b>	Jednoduchá EXE aplikace, která umožňuje aplikaci CROSEUS provádět opakované a přesně specifikované akce.	Oddíl 0	Ne	Server
<b>klientský certifikát určený k podpisu</b>	Musí mít každý uživatel, který chce provádět operace podepisování.	Oddíl 3.3.5	Ne	Koncového uživatele



<b>certifikát softwarového vydavatele DYNATECH</b>	Vyžadován pro malou množinu operací, které umožňují manipulaci s lokálními prostředky klientských stanic (např. podepisování).	Oddíl 3.4	Ne	Klientskou stanicí
<b>Instalátor DYNATECH Installer</b>	Používá se k prvotní instalaci a konfiguraci systému a dále ke každé aktualizaci.	Oddíl 3.8	Ano	Server



Obrázek 2 - Podoba aplikace CROSEUS



### 3.1.1.1 Volitelné adresáře

Aplikace, respektive web CROSEUS může obsahovat jeden, nebo několik volitelných adresářů. To jsou adresáře, které nejsou nezbytnou součástí aplikace, ale pokud existují, zpravidla mají konstantní název i funkci. Nejběžnější z nich jsou:

- Adresář **Msi** – Obsahuje MSI instalátor aplikace Dynatech Signature Tool (viz oddíl 3.3)
- Adresář **Logs** – Obvyklý výstupní adresář pro textové LOG soubory (detaily viz oddíl 3.1.2)
- Adresář **Help** – Obsahuje uživatelskou dokumentaci ve formě HTML, nebo PDF.
- Adresář **zakaznik** – Obsahuje všechny komponenty (např. obrázky a loga), které používá konkrétní zákazník na generovaných PDF dokladech.
- Adresář **WS** – Obsahuje CROSEUS API (více informací viz oddíl 3.1.1.2).

### 3.1.1.2 CROSEUS API

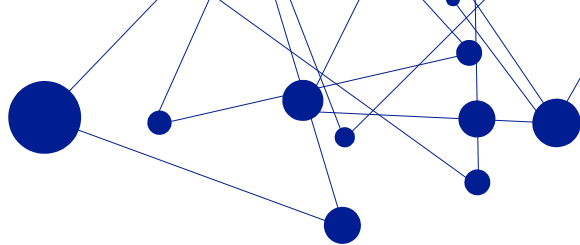
Aplikace, respektive web CROSEUS může volitelně obsahovat komponentu CROSEUS API, což je v podstatě univerzální integrační rozhraní. Toto rozhraní umožňuje dalším externím systémům integrovat se s aplikací CROSEUS, tj. přenášet mezi jednotlivými systémy data. Rozhraní má následující klíčové vlastnosti:

- Je jednosměrné, v současné chvíli umožňuje pouze konzumaci dat (tj. žádná data neodesílá).
- Je na úrovni IIS webu CROSEUS reprezentováno virtuální podaplikací. Dosažitelné je z URL adresy „[\[URL aplikace CROSEUS\]/WS](#)“ (zde je detailní popis řešení i odkaz na WSDL, které je pak použito pro vlastní příjem dat).
- Umožňuje:
  - Přijmout doklad před vznikem závazku (např. Objednávka dodavatelská), po vzniku závazku (Faktura dodavatelská), po vzniku nároku (Faktura odběratelská) včetně příloh.
  - Přijmout pokyn k odeslání dokladu do schvalování.
  - Odpovědět na dotaz ohledně stavu dokladu.
  - Přijmout pokyn k nastavení data úhrady u dokladu.
  - Přejmout organizační strukturu (organizační jednotky, osoby a zařazení osob do organizačních jednotek) z vybraných systémů.
- Podporované jsou následující externí systémy:
  - Dynatech GIS Works – organizační struktura
  - Helios Fenix

K využití integračního rozhraní třetí stranou je třeba se autentizovat jménem/heslem, nebo klientským certifikátem. Identita CROSEUS API musí být na straně serveru zajištěna vlastním serverovým SSL certifikátem (čili musí být hostována na protokolu https).

## 3.1.2 Konfigurace

Prvotní základní konfigurace a nastavení systému CROSEUS se provádí v rámci úvodní instalace za asistence speciální aplikace Dynatech Installer (viz oddíl 3.8). Následné změny základní konfigurace během běžného provozu se pak provádí pomocí úprav:



- v miniaplikaci **Dynatech Settings Manager** – Vestavěná součást aplikace CROSEUS. Umožňuje editaci veškerých základních nastavení aplikace (např. připojení k databázi, vlastnosti notifikačních mailů, vazbu na reporty atd.)
- v souboru **Web.config** v root adresáři webu – Konfigurační soubor IIS webu. Obsahuje některá nastavení týkající se chování IIS (např. způsob autentizace)

Soubory i miniaplikace jsou součástí webu. Miniaplikace je dostupná z URL „[\[URL aplikace CROSEUS\]/settings](#)“. Důležité klíče a jejich význam – viz tabulky v příslušných podkapitolách.

Pokud je součástí řešení i volitelná součást CROSEUS API, tak:

- a) je nejdříve nutné ji aktivovat. Bez toho není možné integraci využít/konfigurovat. Aktivaci provádí na objednávku dodavatel software.
  - a. Aktuální stav aktivace je možné ověřit v „Nastavení“ -> „Nastavení integračních bodů“ -> „Import dokladů pomocí webové služby“, kde hodnoty ve sloupcích „Nasazeno“ a „Aktivní“ musí být nastaveny na „Ano“.
- b) Externímu systému, který se chce s aplikací CROSEUS integrovat, musí být přidělen jedinečný login a heslo, nebo přístupový certifikát. Údaje systému umožní spojit se s aplikací CROSEUS a předat ji svá data.
  - a. Loginy a hesla (formou hash kódu) musí být uložena v databázi CROSEUS, v tabulce „`integrace.EXTERNI_SYSTEM`“.<sup>1</sup>
  - b. Přístupový certifikát musí být včetně privátního klíče k dispozici externímu systému, a tento jej musí umět využít k autentizaci.
- c) v souboru **Web.config** v adresáři „WS“ musí být uveden otisk certifikátu umožňující externímu systému ověřit identitu serveru (viz oddíl 3.1.2.1.1).

Rozšířená konfigurace aplikace CROSEUS (tj. správa uživatelů, konfigurace vnitřní autentizace, odesílání emailů, nastavení vlastností časových známek, úlohy Dynatech scheduleru atd.) se již provádí pomocí voleb na speciálních formulářích, které jsou součástí uživatelského rozhraní (GUI) aplikace – detaily viz uživatelská dokumentace systému.

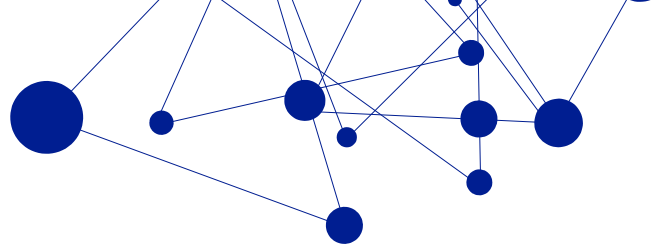
### 3.1.2.1 Dynatech Settings Manager

Miniaplikace je prezentována formou jednoduché webové stránky, na které jsou k dispozici tlačítka zpřístupňující jednotlivé konfigurační oblasti aplikace CROSEUS. Konkrétně jsou k dispozici následující tlačítka:

- **Nastavení aplikace** – zpřístupní základní konfiguraci aplikace CROSEUS. Detaily viz oddíl 3.1.2.1.1
- **Integrace s externími systémy** – v této části se zřizuje/povoluje přístup konkrétních instancí externích systémů ke CROSEUS API. Detaily viz oddíl 3.1.2.1.2

---

<sup>1</sup> Správné naplnění tabulky řeší dodavatel software předáním/aplikací speciálního konfiguračního SQL skriptu. V současné chvíli k této funkcionalitě bohužel neexistuje žádné použitelné GUI.



- **Datové úložiště souborů** – umožňuje nastavit přesun souborů z archivu z databáze CROSEUS do externího úložiště (typ souborový systém) a naopak. Tato funkce dokáže značně zmenšit velikost databáze a tedy celý systém dále provozovat na bezplatné verzi MSSQL serveru.
- **Log** – zobrazí detailní výpis chyb, které systém CROSEUS během svého života zachytí. Které chyby systém zachytává lze ovlivnit pomocí parametru „LogZavaznost“, viz oddíl 3.1.2.1.1.
- **Instalační parametry** – umožňuje administrátorovi systému jednoduše a na jednom místě zobrazit parametry prostředí, nastavené v jednotlivých CONFIG souborech webu CROSEUS.
- **Odhlásit** – umožňuje ihned uzavřít session přihlášeného uživatele.
- **Změnit heslo** – umožňuje změnit heslo přihlášeného uživatele.

Přístup k miniaplikaci je chráněn samostatnou autentizací. Defaultní přihlašovací údaje jsou:

- Login: *admin*
- Heslo: *[prázdné]*

Heslo je možné (**a při prvotní konfiguraci důrazně doporučené**) změnit, login nikoliv.

### 3.1.2.1.1 Nastavení aplikace

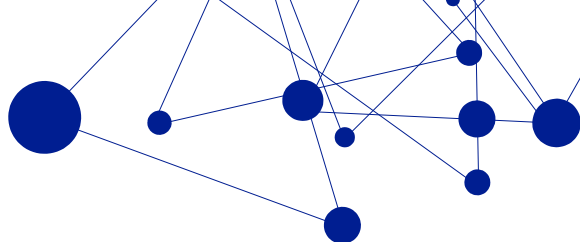
Rozhraní se skládá z přehledu nastavení aplikace CROSEUS a dále pak z tlačítek:

- Hlavní strana – návrat na základní rozcestník
- Uložit – uloží aktuální nastavení do databáze CROSEUS
- Export – uloží aktuální nastavení do externího ZIP souboru
- Import – načte nastavení z externě uloženého ZIP souboru

Jednotlivá nastavení:

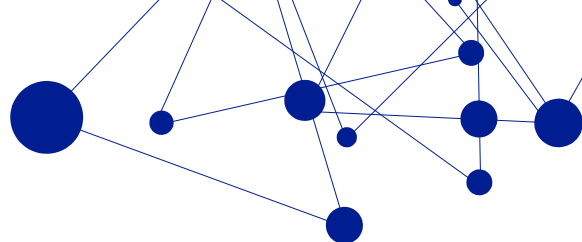
Položka	Oblast	Význam
<b>ConnectionStrings</b>	Databáze	Connection string k databázi CROSEUS. <sup>2</sup>
<b>DefaultTransactionIsolationLevel</b>	Foundation	Upravuje způsob zaznamenávání změn do databáze. Klíč musí být nastaven na hodnotu „Snapshot“.
<b>EmailCustomSmtptFQDN</b>	Foundation	Pokud aplikační server není v doméně, lze vyplnit vlastní FQDN, které bude doplněno v hlavičkách odchozích emailů. Defaultní hodnota je prázdná. <i>POZOR: Při změně nastavení je třeba provést IIS reset.</i>
<b>EmailFrom</b>	Foundation	Doplňuje se do notifikačních emailů jako adresa odesílatele. Není-li uvedena, použije se adresa <a href="mailto:dynatech@dynatech.cz">dynatech@dynatech.cz</a> .
<b>EmailSmtptHost</b>	Foundation	FQDN, nebo IP adresa SMTP serveru.

<sup>2</sup> Je doporučeno uvést i parametr „Connect Timeout“ nastavený na hodnotu „600“.



<b>EmailSmtPassword</b>	Foundation	Heslo k SMTP účtu
<b>EmailSmtPort</b>	Foundation	Číslo portu, na kterém SMTP server naslouchá.
<b>EmailSmtSecure</b>	Foundation	Typ zabezpečení smtp. Možné hodnoty: ssl   tls   prazdne
<b>EmailSmtUsername</b>	Foundation	Uživatelské jméno smtp účtu. Typicky je to email nebo první část emailu před zavináčem.
<b>CustomerId</b>	Core	Jedinečný identifikátor zákazníka, který má vliv na způsob aktualizace databáze. Parametr nelze měnit.
<b>HelpUrl</b>	Core	URL link (nebo lokální cesta) k nápovědě aplikace.
<b>LogZavaznost</b>	Core	Úroveň podrobnosti logování. Čím vyšší, tím větší podrobnost. Povolený rozsah hodnot je 0-1000. Hodnota 0 se rovná stavu „logování je vypnuto“. Tato je defaultní.
<b>MaxAttachmentFileSize</b>	Core	Maximální povolená velikost (v MB) jedné přílohy v rámci jednoho záznamu v aplikaci. Defaultní hodnota je 40 MB.
<b>MaxAttachmentSumSize</b>	Core	Maximální povolená velikost (v MB) všech příloh v rámci jednoho záznamu v aplikaci. Defaultní hodnota je 40 MB.
<b>MinIsolatedStorageSize</b>	Core	Pomocí této hodnoty lze explicitně zvýšit maximální povolenou kapacitu lokálního úložiště Silverlight části aplikace. Pokud je nastavena hodnota vyšší než 0, pak je vhodné zvýšení kvóty rovněž explicitně povolit. <sup>3</sup> V případě, že zvýšení kvóty explicitně povoleno není, pak každý uživatel může zvýšení kvóty povolit manuálně. A to kliknutím na tlačítko „ANO“ v dialogu, který se zobrazí při prvním startu aplikace Croseus. Hodnota je v bajtech. Výchozí hodnota je 0.
<b>RemoteManagement</b>	Core	Povoluje/zakazuje vzdálený management hodnot Dynatech settings managera. Defaultní hodnota je „Ne“. Ke správné funkci musí být v aplikaci CROSEUS zprovozněno CROSEUS API.
<b>ReportingEmailFrom</b>	Core	Emailová adresa odesílatele, která bude uvedena v každém odchozím emailu informujícím o výskytu chyby.
<b>ReportingEmailSubject</b>	Core	Definuje obsah pole „předmět“ v každém emailu informujícím o výskytu chyby v aplikaci.

<sup>3</sup> Postup je dostupný např. na adrese: [http://support.dundas.com/Dashboard5.Application\\_Storage.ashx](http://support.dundas.com/Dashboard5.Application_Storage.ashx)

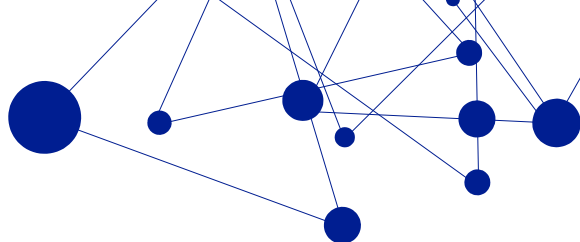


<b>ReportingEmailTo</b>	Core	Seznam emailových adres, na něž se odešle email s přesným chybovým hlášením vždy, pokud v aplikaci k nějaké chybě dojde. Pokud seznam neobsahuje žádnou adresu, neodešle se žádný email.
<b>ReportingLogDir</b>	Core	Relativní, nebo absolutní cesta k adresáři, ve kterém mohou vznikat log soubory aplikace. Není-li cesta uvedena, budou log soubory vytvářeny přímo v kořenovém adresáři aplikace.
<b>ReportingLogFilename</b>	Core	Určuje společný název všech log souborů, které vznikají za běhu aplikace. Aplikace tento název ještě vždy rozšíří o datum vzniku každého jednotlivého souboru.
<b>RozcestnikURL</b>	Core	Odkaz na libovolný rozcestník. Rozcestník je jednoduchá webová stránka, kde jsou uvedené odkazy na dostupné aplikace rodiny CROSEUS v rámci celé organizace. Tento odkaz bude dostupný v zápatí aplikace CROSEUS Online. Doporučujeme použít absolutní URL. Vý-chozí hodnota je prázdná.
<b>CROSEUS API – Server authenticate certificate (Thumbprint)</b>	Core	Vazba na certifikát, který poslouží externím systému k ověření identity serveru, na kterém je provozována komponenta CROSEUS API. Zapsaná hodnota musí být shodná s vlastností „Thumbprint“ cílového certifikátu. <sup>4</sup> <i>POZOR: Tato položka není součástí exportu nastavení!</i>
<b>ApplicationName</b>	DFS	Titulek aplikace CROSEUS. Pokud není uvedeno, použije se defaultní hodnota „Dynatech Form Systems“
<b>AresRespondCache<sup>5</sup></b>	DFS	Nastavení určuje způsob interakce se systémem ARES. Může nabývat hodnot: <ul style="list-style-type: none"> <li>• Disable = Nepoužívá se lokální cache. Systém komunikuje přímo s ARES.</li> </ul>

<sup>4</sup> Nastavení certifikátu je možné měnit např. pomocí nástroje DYNATECH Certificate Picker, který je dostupný v adresáři webové služby CROSEUS API. Certifikát musí být vhodný pro podepisování (tj. Key Usage=Digital Signature, součástí je privátní klíč) a musí být uložen v "Certificate Store/Local Machine/Personal". Ke správné funkci aplikace Certificate Picker vyžaduje právo čtení z "Local Machine Certificate Store" a práva čtení, zápis a editace nad souborem "web.config" (v adresáři "WS").

<sup>5</sup> Aktuální stav RespondCache lze vidět přímo v aplikaci CROSEUS v sekci „Nastavení“ -> „Integrace“ -> „ARES RespondCache“

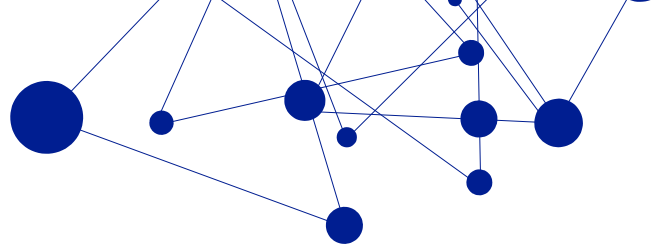




		<ul style="list-style-type: none"> <li>• Only Log = Nepoužívá se lokální cache. Systém komunikuje přímo s ARES + každou odpověď uloží do logu.</li> <li>• Enable = Používá se lokální cache. Pokud zde právě hledaný záznam není, kontaktuje se ARES.</li> <li>• Use Only Cache = Používá se pouze lokální cache. Defaultně je prázdná. Defaultní hodnota klíče je "Use Only cache". Doporučená pro ostrý provoz je hodnota "Disable".</li> </ul>
<b>AresSoapServiceAdresa</b>	DFS	URL adresa na aktuální ministerstvem financí provozovanou webovou službu ARES (SOAP endpoint). <sup>6</sup> Doporučená hodnota je: <a href="http://wwwinfo.mfcr.cz/cgi-bin/ares/xar.cgi">http://wwwinfo.mfcr.cz/cgi-bin/ares/xar.cgi</a>
<b>DanovyPortalAdresa</b>	DFS	URL adresa na aktuální ministerstvem financí provozovanou webovou službu pro zjišťování spolehlivosti plátců DPH. <sup>7</sup>
<b>DST</b>	DFS	URL, nebo lokální cesta k aktuálnímu instalačnímu souboru aplikace DST.
<b>TitleBarBackground</b>	DFS	Barva textu záhlaví aplikace CROSEUS. Pokud není uvedeno, bude text tmavě šedý.
<b>TitleBarForeground</b>	DFS	Barva pozadí záhlaví aplikace CROSEUS. Pokud není uvedeno, bude pozadí bílé.
<b>ApplicationURL</b>	Dynatech Scheduler	URL adresa aplikace CROSEUS.
<b>Adresář se soubory s chybou</b>	Integrace ze sdíleného adresáře	Určuje adresář, kam aplikace přesune exportované soubory z EIS, kde došlo při importu k chybě. Očekává se síťový adresář.
<b>Adresář se soubory k automatickému importu</b>	Integrace ze sdíleného adresáře	Určuje adresář, kde aplikace očekává exportované soubory z EIS. Očekává se síťový adresář.
<b>Adresář se soubory k manuálnímu importu</b>	Integrace ze sdíleného adresáře	Určuje adresář, kde aplikace očekává exportované soubory z EIS, k dodatečnému manuálnímu importu. Očekává se síťový adresář.
<b>CIM - Url</b>	Dynatech Auth Provider	URL k poskytovateli identit (CIM). Pokud není vyplněno, aplikace není s CIM integrována. Výchozí hodnota je prázdná. Doporučovaný

<sup>6</sup> Více informací viz [http://wwwinfo.mfcr.cz/ares/xml\\_doc/schemas/index.html](http://wwwinfo.mfcr.cz/ares/xml_doc/schemas/index.html), odkaz „basic.wsdl“.

<sup>7</sup> Aktuální informace viz [http://adisspr.mfcr.cz/adistc/adis/idpr\\_pub/dpr\\_info/ws\\_spdph.faces](http://adisspr.mfcr.cz/adistc/adis/idpr_pub/dpr_info/ws_spdph.faces).



		postup připojení k CIM: zadat adresu k CIM a kliknout na Registrovat. Po zadání údajů pro CIM budou hodnoty vyplněny na obou stranách.
<b>Identifikátor aplikace</b>	Dynatech Auth Provider	Identifikátor aplikace vůči poskytovateli identit.
<b>Klíč aplikace</b>	Dynatech Auth Provider	Sdílené tajemství s poskytovatelem identit.
<b>Insights Id</b>	Cloud	Zapíná, nebo vypíná monitorování aplikace pomocí služby Azure Insights.

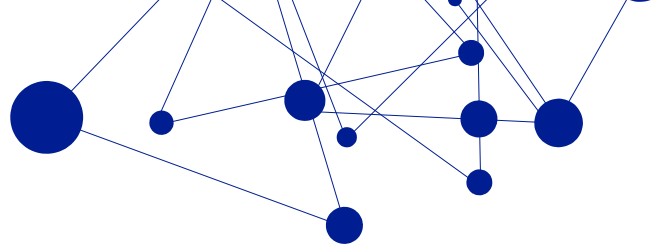
### 3.1.2.1.2 Integrace s externími systémy

Rozhraní se skládá z přehledu evidovaných externích systémů a jim přidělených vlastností (vlastnosti lze editovat přes odkaz „Zobrazit“) a dále pak z tlačítek:

- Hlavní strana – návrat na základní rozcestník
- Nový – umožňuje založit nový záznam. Na tomto formuláři jsou k dispozici další tlačítka:
  - Seznam – návrat zpět na přehled evidovaných externích systémů
  - Uložit – uloží aktuálně editovaný záznam
  - Odstranit – trvale smaže aktuálně editovaný záznam

Každý záznam obsahuje následující informace:

Vlastnost	Hodnota
<b>Název</b>	Identifikátor externího systému. Musí být jedinečný.
<b>Aktivní</b>	Volba Ano/Ne. Určuje, zda externímu systému bude povolen přístup ke CROSEUS API, nebo nikoliv. Defaultní hodnota je „Ne“.
<b>Popis</b>	Volitelné doplňující informace.
<b>Přístupové jméno</b>	Login, který může externí systém využít k přihlášení.
<b>Přístupové heslo</b>	Heslo, které může externí systém využít k přihlášení.
<b>Přístupové heslo2</b>	Heslo, které může externí systém využít k přihlášení.
<b>Přístupový certifikát Thumprint</b>	Certifikát, který může externí systém využít k přihlášení.
<b>Přístupový certifikát Thumprint2</b>	Certifikát, který může externí systém využít k přihlášení.
<b>Validovat klientský certifikát</b>	Volba Ano/Ne. Určuje, zda se u certifikátu budou ověřovat jeho vlastnosti ve smyslu jeho aktuální platnosti.



### 3.1.2.1.3 Datové úložiště souborů

Výsledkem schvalovacích postupů v aplikaci CROSEUS jsou PDF doklady. PDF doklady jsou archivovány buď přímo v databázi CROSEUS, nebo (volitelně) v souborovém systému. Jako výchozí je nastaveno archivování v databázi. Rozhraní se skládá z několika funkčních tlačítek:

- Aktivovat přesun – provede rekonfiguraci aplikace CROSEUS. PDF doklady se budou od této chvíle ukládat do zvoleného umístění v souborovém systému. Pro správnou funkci je třeba nastavit vlastnost „Adresář s archivovanými soubory“ (viz níže).
- Zrušit přesun – provede rekonfiguraci aplikace. PDF doklady se budou od této chvíle ukládat do databáze CROSEUS.
- Po rekonfiguraci aplikace proběhne dodatečná migrace již existujících dokladů do vybraného typu úložiště. Migraci je možné ihned manuálně vynutit tlačítkem „Spustit“, nebo se provede později jako aktivita v aplikaci Dynatech Scheduler (viz oddíl 0).

Konfigurovatelné vlastnosti:

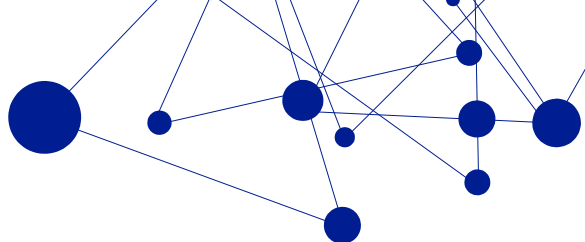
Vlastnost	Hodnota
Adresář s archivovanými soubory	Cesta do adresáře, do něž se budou ukládat archivované soubory. <sup>8</sup>

Nad archivovanými doklady je nutné mít nastaven proces zálohování, buď jako součást zálohování databáze, nebo nově jako zálohování zvoleného adresáře (viz kapitola 4).

### 3.1.2.2 Web.config v root adresáři

Klíč	Nadřazený klíč	Význam
Authentication mode="[klíčové_slovo]"	system.web	Je-li obsahem slovo „ <b>Windows</b> “, klíč vynucuje autentizaci uživatelů pomocí windows/AD účtů. Je-li obsahem slovo „ <b>Anonymous</b> “, klíč vynucuje autentizaci uživatelů pomocí speciálních účtů aplikace CROSEUS. Není-li klíč uveden vůbec, zdědí se nastavení z webu vyšší úrovně, případně z nastavení root IIS.
Allow roles="[AD_skupiny]"	authorization	Obsahuje seznam AD skupin a uživatelů, kteří mají k aplikaci povolený přístup. Lze použít znak „*“ pro všechny osoby. Nastavení se týká omezení přístupu na úrovni IIS.
Deny users="[AD_uživatelé]"	authorization	Obsahuje výpis uživatelů, kteří přístup nemají. Pokud je nějaký uvedený v klíči „Allow roles...“, nastavení se pro něj ignoruje. Lze použít znak „*“ pro všechny osoby. Nastavení se týká omezení přístupu na úrovni IIS.

<sup>8</sup> Aplikace CROSEUS předpokládá, že zvolený adresář existuje a že nad ním má příslušná oprávnění – viz oddíl 3.5.4



### 3.1.3 Instalační postupy

Aplikace CROSEUS se nasazuje do IIS (což je volitelná součást operačního systému Windows). Nasazení lze provést:

1. Automaticky – Nasazení provádí kompletně dodavatel software, firma DYNATECH, pomocí svých vlastních interních nástrojů.
2. Polo-automaticky – většinu prerekvizit a instalačních procedur administrátor organizace nasadí/provede pomocí průvodce (speciální aplikace Dynatech Installer). Jedná se o preferovanou variantu.
3. Manuálně – Administrátor si celé prostředí pro běh systému připraví sám. Tato varianta je vhodná pro prostředí se specifickými, nebo striktně kontrolovanými vlastnostmi provozního prostředí.

Zvolený způsob instalace i upgrade lze kdykoliv nahradit některou z ostatních variant.

#### 3.1.3.1 Automatické nasazení

##### 3.1.3.1.1 První nasazení

Provádí na zakázku přímo dodavatel software, firma DYNATECH.

##### 3.1.3.1.2 Upgrade

Proces aktualizace celého systému CROSEUS je řízen centrálně a prováděn na objednávku a to v pravidelných intervalech.

#### 3.1.3.2 Polo-automatické nasazení

##### 3.1.3.2.1 První nasazení

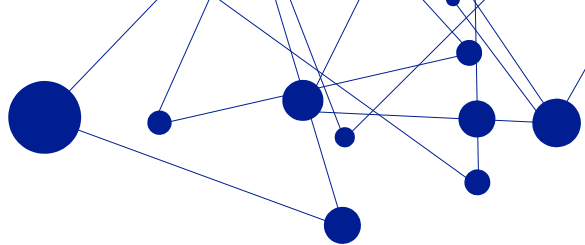
1. Získáme instalační ZIP balíček od dodavatele, tj. firmy DYNATECH.
2. Na zvoleném IIS serveru balíček rozbalíme a nainstalujeme prerekvizity pro běh aplikace Dynatech installer – viz oddíl 3.8.5.
3. Spustíme instalátor Dynatech installer, vyplníme a zkontrolujeme instalační parametry a spustíme vlastní instalaci – detaily viz oddíl 3.8.3.
4. Počkáme na dokončení instalace.
5. Provedeme úvodní konfiguraci aplikace pomocí změn v miniaplikaci Dynatech Settings Manager (viz oddíl 3.1.2).

##### 3.1.3.2.2 Upgrade

1. Získáme instalační ZIP balíček od dodavatele, tj. firmy DYNATECH.
2. Aktualizujeme aplikaci CROSEUS pomocí speciálního průvodce, tj. aplikace Dynatech Installer – více informací viz oddíl 3.8. Aktualizaci vykonává zvolený správce aplikace.

#### 3.1.3.3 Manuální nasazení

##### 3.1.3.3.1 První nasazení



Při manuálním nasazení se aplikace CROSEUS nasazuje do IIS stejně, jako kterýkoliv jiný běžný IIS web. Je více než vhodné vytvořit pro ni samostatný aplikační pool s vlastním účtem tak, aby byla aplikace odizolována od ostatních procesů v systému (a případně bylo možné definovat na dalších navazujících službách oprávnění specifická právě pro ni). Vzhledem k rozmanitosti prostředí a jednotlivých instalací IIS nelze napsat na tuto část dostatečně univerzální manuál. U administrátora, který nasazení provádí, se proto předpokládá alespoň elementární znalost IIS a principů jeho fungování.<sup>9</sup> Obecně lze nasazení aplikace CROSEUS popsat takto:

1. Na zvoleném serveru ve vhodné části souborového systému (defaultně „C:\inetpub\“) vytvoříme nový adresář (např. „CROSEUS“).
2. Do něj umístíme soubory webové služby (soubor ASPX, adresář „bin“ s DLL knihovny atd. Součástí jsou i soubory „\*.config“).
3. Doplníme volitelné adresáře (seznam bývá zpravidla specifikován v rámci nasazení) – viz oddíl 3.1.1.1.
4. Přidání aplikace do IIS potom probíhá stejně jako přidání „virtuálního adresáře“ do existujícího, nebo nového webu v IIS. Díky tomu, že přidáme virtuální adresář odkazující na adresář, ve kterém je obsažen soubor „web.config“, vytvoří se virtuální adresář jako samostatná webová aplikace, u které je následně možné nastavit aplikační pool. Ve vlastnostech aplikačního poolu se nastavuje identita, pod kterou celá aplikace běží. Aplikační pool i virtuální adresář musí splňovat určitá kritéria – viz oddíl s popisem konfigurace.
5. Pokud je součástí aplikace i adresář „WS“, musí být tento následně:
  - a. nastaven jako „virtuální aplikace“,
  - b. typ autentizace je na tomto uzlu třeba nastavit pouze na hodnotu „Anonymous Authentication“.
6. Přes příkazovou řádku provedeme na serveru restart IIS služby (příkaz „iisreset“).
7. Provedeme úvodní konfiguraci aplikace pomocí změn v CONFIG souborech a miniaplikace Dynatech Settings Manager (viz oddíl 3.1.2).
8. Pokud nasazujeme více instancí aplikace CROSEUS (např. produkční a verifikační verzi), můžeme je umístit na stejný web. Hierarchicky však musí být umístěny jednotlivé aplikace vedle sebe, nikoliv za/pod sebou. Taková konfigurace není podporována.

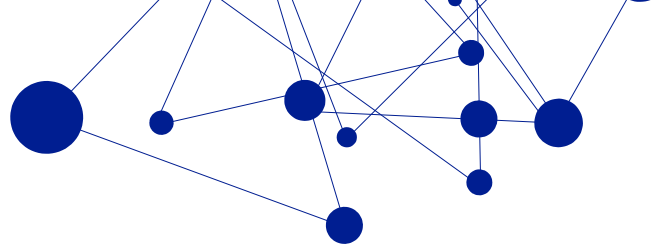
### 3.1.3.3.2 Upgrade

1. Aktualizace aplikace CROSEUS probíhá formou nahrazení původních souborů aplikace ve filesystému soubory nové verze (jedná se tedy o jednoduchou operaci Copy&Paste). Během operace doporučujeme zachovat volitelné adresáře a jejich obsah (viz oddíl 3.1.1.1). Tato instrukce neplatí pro adresář „WS“.
2. Po úspěšném nahrazení souborů provedeme na aplikačním serveru restart IIS služby (příkaz „iisreset /noforce“).



**POZOR:** Tento typ aktualizace již není plně podporován. Popis tak nemusí obsahovat všechny kroky nezbytné k úplnému dokončení procesu aktualizace na vyšší verzi.

<sup>9</sup> Firma Dynatech s.r.o. dodává ke každému prvnímu nasazení aplikace dostatečně podrobný step-by-step návod, který umožňuje uvést produkt do 100% funkčního stavu i bez pokročilých znalostí.



### 3.1.3.4 Ověření prerekvizit na straně klienta

O prerekvizitách na straně klientských stanic a jejich instalaci pojednávají samostatné pododdíly 3.1.5.2 a 3.1.5.3. Aplikace CROSEUS však nabízí koncovým uživatelům nástroj, kterým lze na každé jednotlivé stanici ověřit, zda splňuje potřebná kritéria. A to online a v reálném čase.

Nástroj je dostupný na URL „[\[URL aplikace CROSEUS\]/verify](#)“.



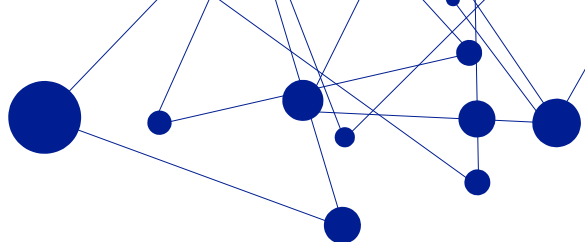
CROSEUS		
Ověřovací stránka		
1. Silverlight:	✓	min. 5.1.10411.0
2. CROSEUS:	✓	1.2.2.6392
3. Elevated permission:	✓	
4. Dynatech Signature Tool:	✓	1.9.0.x
5. Elektronický podpis:	✗	<input type="button" value="Vybrat"/>

Obrázek 3 - Podoba ověřovací stránky aplikace CROSEUS

### 3.1.4 Potřebná oprávnění

a) Účet, pod kterým běží aplikační pool, musí:

- Být členem lokální skupiny „IIS\_IUSR“ (nebo „IIS\_WPG“) na serveru, kde je aplikace nasazena.
- Vystupovat v rolích „log on as a service“ a „log on as a batch job“ v lokálních bezpečnostních politikách aplikačního serveru.
- Mít serverovou roli „public“ na SQL serveru, kde je provozována databáze CROSEUS.
- Nad databází CROSEUS mít role: public a db\_systemaccount.
- Nad adresářem, ve kterém se ukládají log soubory aplikace (standardně adresář „Logs“, který je součástí serverové části silverlight aplikace CROSEUS), mít práva: Read, Write, Modify, Read&Execute a List Folder Content.
- Na adresáři „%systemroot%\TEMP“ na serveru, kde je aplikace nasazena, mít práva: Read, Write, Read&Execute a List Folder Content.
- Mít přístup k SMTP serveru za účelem odesílání informačních emailů

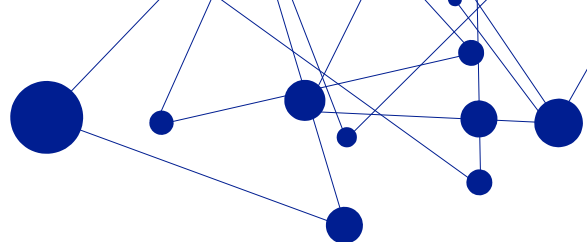


- (volitelně) Mít přístup ke službě (certifikační autoritě) vydávající kvalifikovaná časová razítka (např. [www.postsignum.cz](http://www.postsignum.cz)). Aplikace CROSEUS umí pracovat s následujícími metodami přístupu:
    - i. [doporučené] pomocí přístupového certifikátu ke službě/certifikační autoritě, který je uložen v operačním systému aplikačního serveru, konkrétně v osobním úložišti certifikátů pro účet aplikačního poolu<sup>10</sup>. Aplikace CROSEUS certifikát identifikuje na základě hodnoty „Subject Key Identifier“. Certifikát musí obsahovat privátní klíč.
    - ii. pomocí přístupového certifikátu ke službě/certifikační autoritě, který je uložen v databázi CROSEUS (konkrétně v tabulce CZ\_POSKYTOVA-TELE\_CASOVEHO\_RAZITKA)
    - iii. pomocí jména a hesla uživatelského účtu zřízeného u služby/certifikační autority
    - iv. přímý přístup ke službě/certifikační autoritě bez autentizace (umožňuje-li to)
  - (volitelně) Mít přístup k internetu, konkrétně k adrese:
    - i. <http://adisrws.mfcr.cz:80> – využívá se k ověření, zda subjekt užitý v procesu řídicí kontroly je spolehlivým plátcem DPH.
- b) IIS web, respektive virtuální adresář, kde je aplikace nasazena, musí mít:
- a. IIS oprávnění „Read“ a „Run scripts (such as ASP)“.<sup>11</sup>
  - b. Způsob autentizace nastaven:
    - i. pouze na hodnotu „Windows Authentication“, chceme-li, aby se uživatelé autentizovali pomocí windows/AD účtů.
    - ii. pouze na hodnotu „Anonymous Authentication“, chceme-li, aby se uživatelé autentizovali pomocí speciálních účtů aplikace CROSEUS.
  - c. (volitelně) Je vhodné zajistit, aby web/virtuální adresář blokoval požadavky na manipulaci s obsahem typu EXE, respektive aby neposkytoval běžným uživatelům přímý přístup k souborům Dynatech Scheduleru (popis komponenty viz oddíl 0).
    - i. To lze zajistit např. úpravou vlastností webu, konkrétně seznamu „Request Filtering“ – „File Name Extensions“. Stačí, když do tohoto seznamu pomocí akce „Deny File Name Extensions...“ vložíme hodnotu „.exe“. Detaily viz. <http://technet.microsoft.com/cs-cz/library/hh831621.aspx>.
- c) Koncoví uživatelé musí mít možnost spouštět Silverlight aplikace v módu zvýšené důvěry<sup>12</sup> – tzn. typicky musí mít na svých pracovních stanicích v registrech operačního systému nastaven:
- a. Klíč „AllowElevatedTrustAppsInBrowser“ nacházející se ve větvi „HKEY\_LOCAL\_MACHINE\Software\Microsoft\Silverlight“ na hodnotu „1“ typu DWORD (u 32bit operačních systémů).

<sup>10</sup> Certifikát může být uložen i v osobním úložišti certifikátů lokálního počítače (na aplikačním serveru). V takovém případě je ale třeba účtu aplikačního poolu explicitně udělit právo „read“ pro přístup k privátnímu klíči (např. prostřednictvím metody „All tasks“ --> „Manage Private Keys...“).

<sup>11</sup> U IIS verze 7.0 a vyšší je toto nastavení defaultní.

<sup>12</sup> Kvůli možnosti vkládat do systému přílohy z lokálního počítače, či podepisovat dokumenty/doklady.



- b. Klíč „AllowElevatedTrustAppsInBrowser“ nacházející se ve větvi „HKEY\_LOCAL\_MACHINE\Software\Wow6432Node\Microsoft\Silverlight\“ na hodnotu „1“ typu DWORD (u 64bit operačních systémů).
- c. Klíč je možné u uživatelů hromadně nastavovat např. prostřednictvím Active Directory politik. Detailní postup viz <http://technet.microsoft.com/en-us/library/cc753092.aspx>. U moderních verzí GPO lze pro rozlišení stanic s 32bit/64bit OS využít postup popsany na <http://technet.microsoft.com/en-us/library/cc733022.aspx>. U starších verzí GPO se musíme spolehnout na WMI filtry (query „Select \* from Win32\_Processor where AddressWidth = '64' “). Detaily viz [http://technet.microsoft.com/en-us/library/cc779036\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc779036(WS.10).aspx).

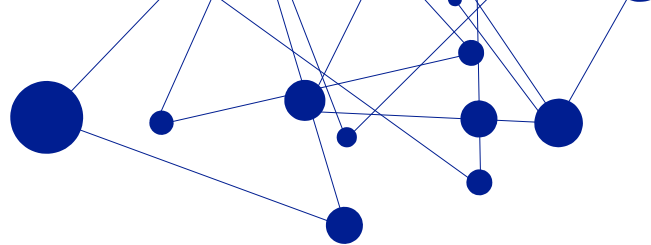
### 3.1.5 Minimální HW a SW nároky

#### 3.1.5.1 Server

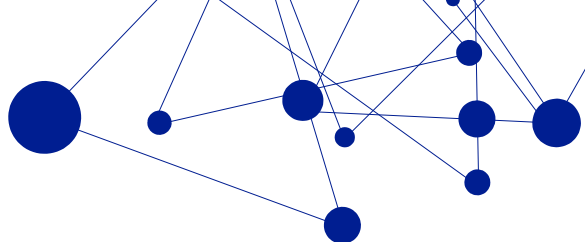
- HW konfigurace:
  - ≤10 uživatelů: více jádrový 2GHz CPU, 4 GB RAM, 100 Mbit/s NIC
  - ≤100 uživatelů: více jádrový 2GHz CPU, 4 GB RAM, 1 Gbit/s NIC
  - >100 uživatelů: více jádrový 2GHz CPU, 8 GB RAM, 10 Gbit/s NIC
- Microsoft .NET Framework 4.7.1 nebo vyšší
  - <http://go.microsoft.com/fwlink/?linkid=852107>
  - Pro vyšší spolehlivost aplikace důrazně doporučujeme nainstalovat také opravu pro Microsoft operační systémy – KB2977218:  
<https://www.microsoft.com/en-us/download/details.aspx?id=43687>
- IIS verze 7 a vyšší
- IIS web, nebo virtuální adresář podporující ASP.NET verze 4.0 a vyšší
  - IIS web musí být přístupný prostřednictvím protokolu HTTPS
  - Musí podporovat MIME typ „application/x-silverlight-app“ (přípona „.xap“)<sup>13</sup>
  - Musí podporovat „FastCgiModule“ v „Handler Mappings“ pro \*.php soubory
  - IIS aplikační pool musí mít vlastnost „Load User Profile“ nastavenou na „True“
- Požadavky na role a rysy operačního systému (tj. co musí být nainstalováno):
  - Role:
    - Application Server
      - .NET Framework 4.5
      - COM+ Network Access
      - TCP Port Sharing
      - Web Server (IIS) Support

<sup>13</sup> U IIS verze 7.0 a vyšší je toto nastavení defaultní.





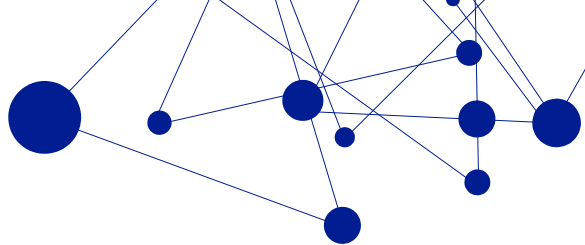
- Windows Process Activation Service Support
  - HTTP Activation
  - Message Queuing Activation
  - Named Pipes Activation
  - TCP Activation
- Web Server
  - Common HTTP Features
    - Default Document
    - Directory Browsing
    - HTTP Errors
    - Static Content
    - HTTP Redirection
  - Health and Diagnostics
    - HTTP Logging
    - Logging Tools
    - Request Monitor
    - Tracing
  - Performance
    - Static Content Compression
    - Dynamic Content Compression
  - Security
    - Request Filtering
    - Basic Authentication
    - Client Certificate Mapping Authentication
    - Digest Authentication
    - IIS Client Certificate Mapping Authentication
    - IP and Domain Restrictions
    - URL Authorization
    - Windows Authentication
  - Application Development
    - .NET Extensibility 3.5
    - .NET Extensibility 4.5
    - ASP
    - ASP.NET 3.5
    - ASP.NET 4.5



- CGI
- ISAPI Extensions
- ISAPI Filters
- Management Tools
  - IIS Management Console
  - IIS Management Scripts and Tools
  - Management Service
- Rysy:
  - Windows Process Activation Service
    - Process Model
    - Configuration APIs
- Microsoft Silverlight klient 5.1.10411.0 a vyšší
  - <http://www.microsoft.com/getsilverlight/>
- Microsoft ODBC driver 11 for SQL server nebo novější
  - <https://www.microsoft.com/en-us/download/details.aspx?id=36434>
- Microsoft C++ Redistributable for Visual Studio 2012 Update 4
  - <https://www.microsoft.com/en-us/download/details.aspx?id=30679>
- Následující prerekvity instalované přes Web Platform Installer 5.0<sup>14</sup>
  - PHP 5.6.x (kde x >= 16)
  - Windows Cache Extension 1.3 for PHP 5.6
  - Microsoft Drivers 3.2 for PHP v5.6 for SQL Server in IIS
  - URL Rewrite 2.0
- V konfiguraci PHP musí být, oproti defaultní konfiguraci, povoleny moduly<sup>15</sup>:
  - `extension=php_fileinfo.dll`
  - `extension=php_intl.dll`
- Volný port, na kterém lze aplikaci zpřístupňovat (na serveru, kde je nasazena)
- (volitelně) Přístupový certifikát, nebo login a heslo, pro přístup ke službě/certifikační autoritě vydávající kvalifikovaná časová razítka
- (volitelně) Přístup k internetu za účelem:
  - Získání časového razítka od certifikační autority
  - Ověření spolehlivosti plátců DPH z veřejně dostupného daňového portálu ministerstva financí ČR

<sup>14</sup> K dispozici zde: <https://www.microsoft.com/web/downloads/platform.aspx>

<sup>15</sup> Uvedené moduly jsou součástí základní instalace PHP. Aktivace se provádí zapsáním příslušných řádků kódu do souboru `php.ini` (defaultní umístění „c:\Program Files (x86)\PHP\v5.6\“).



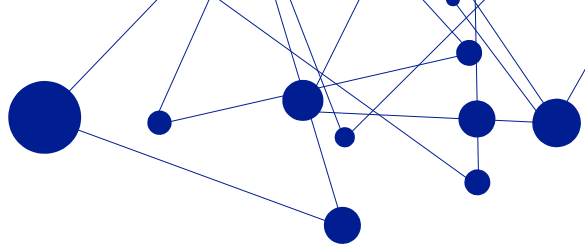
- (volitelně) Pokud je součástí řešení i CROSEUS API (viz oddíl 3.1.1.2):
  - Chce-li externí systém k autentizaci využít přístupový certifikát, musí tento certifikát splňovat následující vlastnosti:
    - Musí obsahovat privátní klíč.
    - Musí být použitelný pro autentizaci, tj. např. v klíčových vlastnostech („key usage“) mít uveden příznak „Client Authentication“.
    - (volitelně) Certifikátu musí aplikace CROSEUS věřit (tj. musí být platný, důvěryhodný atd.).
    - (volitelně) Certifikát nesmí figurovat na revokačním listu certifikační autority, která jej vydala.<sup>16</sup>
- (volitelně) Nastavenou událost ve Windows Scheduleru pro automatické vyvolávání plánovaných akcí (viz samostatný oddíl 0)
- Databáze CROSEUS (viz oddíl 3.2) – nemusí být umístěna lokálně, stačí, když k ní aplikace bude mít přístup

### 3.1.5.2 Klientské stanice bez možnosti podepisovat

- HW konfigurace:
  - Minimální požadavky<sup>15</sup>:
    - Dvoujádrový CPU 1,6GHz Intel Core 2 Duo nebo novější
    - 2 GB RAM (alespoň 512 MB volné paměti)
    - 100 Mbit/s NIC, propustnost sítě ve směru k aplikačnímu serveru alespoň 1 Mb/s
    - rozlišení alespoň 1024x768
  - Doporučená konfigurace:
    - Dvoujádrový CPU 2 GHz Intel Core i3 nebo novější
    - 4 GB RAM (alespoň 1 GB volné paměti) a více
    - Rozlišení 1440x900 a vyšší
- Microsoft Windows 7, 8.1 nebo 10
- Microsoft Silverlight klient 5.1.10411.0 a vyšší
  - <http://www.microsoft.com/getsilverlight/>
- Internet Explorer 11, kompatibilní se Silverlight
  - Kompatibilitu se Silverlight lze kdykoliv ověřit na stránkách <http://www.microsoft.com/getsilverlight/Get-Started/Install/Default.aspx>, v záložce „System Requirements“

<sup>16</sup> Z tohoto důvodu je třeba zajistit, aby aplikace CROSEUS měla přístup k revokačnímu listu dané certifikační autority. Pokud jej nemá, nedokáže 100% ověřit platnost certifikátu a odmítne jej.

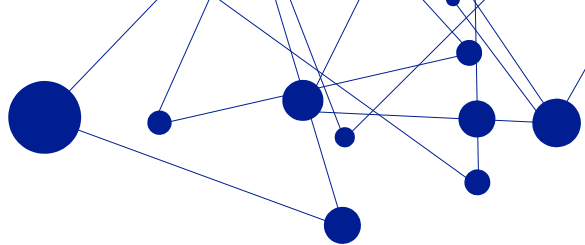
<sup>15</sup> Splnění minimálních požadavků nemusí zajistit rychlý běh aplikace. Aplikace se výrazně zpomaluje při zaplnění paměti RAM, kdy dochází k tzv. swapování (odkládání dat z RAM na pevný disk).



- (volitelně) V případě, že je autentizace typu windows, URL, na kterém je aplikace provozována, musí mít uživatelé zařazeno do zóny „Local intranet“. V opačném případě budou mít značně ztíženu možnost práce s doklady ve formě PDF (každá operace bude vyžadovat nové zadání autentizačních údajů).
- (volitelně) Aby uživatelé mohli provádět operace, které jim umožňují manipulovat s lokálními prostředky klientských stanic (např. vkládat přílohy), musí mít každý z nich uložen na své klientské stanici v úložišti osobních certifikátů v sekci „Trusted Publishers“ certifikát softwarového vydavatele Dynatech. Detaily viz samostatný oddíl 3.4.

### 3.1.5.3 Klientské stanice s možností podepisovat

- HW konfigurace:
  - Minimální požadavky:
    - Dvoujádrový CPU 1,6GHz Intel Core 2 Duo nebo novější
    - 2 GB RAM (alespoň 512 MB volné paměti)
    - 100 Mbit/s NIC, propustnost sítě ve směru k aplikačnímu serveru alespoň 1 Mb/s
    - rozlišení alespoň 1024x768
  - Doporučená konfigurace:
    - Dvoujádrový CPU 2 GHz Intel Core i3 nebo novější
    - 4 GB RAM (alespoň 1 GB volné paměti) a více
    - Rozlišení 1440x900 a vyšší
  - Microsoft Windows 7, 8.1 nebo 10
- Microsoft Silverlight klient 5.1.10411.0 a vyšší
  - <http://www.microsoft.com/getsilverlight/>
- Internet Explorer 11, kompatibilní se Silverlight
  - Kompatibilitu se Silverlight lze kdykoliv ověřit na stránkách <http://www.microsoft.com/getsilverlight/Get-Started/Install/Default.aspx>, v záložce „System Requirements“
- Dynatech Signature Tool (viz samostatný oddíl 3.3) + prekvizity tohoto produktu
- (volitelně) V případě, že je autentizace typu windows, URL, na kterém je aplikace provozována, musí mít uživatelé zařazeno do zóny „Local intranet“. V opačném případě budou mít značně ztíženu možnost práce s doklady ve formě PDF (každá operace bude vyžadovat nové zadání autentizačních údajů).
- Aby uživatelé mohli provádět operace, které jim umožňují manipulovat s lokálními prostředky klientských stanic (např. podepisovat apod.), musí mít každý z nich uložen na své klientské stanici v úložišti osobních certifikátů v sekci „Trusted Publishers“ certifikát softwarového vydavatele Dynatech. Detaily viz samostatný oddíl 3.4.



## 3.2 Databáze CROSEUS

### 3.2.1 Popis

Databáze obsahuje data pro aplikaci CROSEUS.

### 3.2.2 Konfigurace

Databáze CROSEUS je MS SQL databáze, která má následující vlastnosti:

Collation	SQL_Czech_CP1250_CI_AS
Recovery model	Full
Compatibility level	SQL Server 2012 (110), SQL Server 2014 (120), SQL Server 2016 (130) nebo SQL Server 2017 (140)

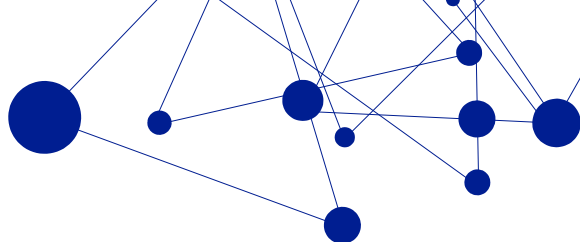
O ostatních vlastnostech se předpokládá, že jsou nastavené defaultně, dle prostředí, ve kterém je databáze nasazena, s následujícími výjimkami:

- Na databázi musí být povolen „snapshot\_isolation\_state“
  - POZNÁMKA: Stav lze kdykoliv ověřit prostřednictvím SQL query:  
`SELECT name, snapshot_isolation_state_desc FROM sys.databases`
- Na databázi musí být nastaven vlastník („Vlastnosti databáze“ -> „Files“), který má na úrovni databáze minimálně práva db\_owner.

### 3.2.3 Instalační postupy

#### 3.2.3.1 První nasazení

1. Na zvolené databázové MS SQL instanci založíme novou databázi libovolného jména (např. „CROSEUS“).
2. Nad novou databází provedeme restore zálohy databáze CROSEUS dodané v rámci prvního nasazení.
  - Klikneme pravým tlačítkem myši nad novou databází.
  - Zvolíme „Tasks“ -> „Restore“ -> „Database...“
  - Zatrhneme možnost „(o) From device“ a navolíme zálohu databáze CROSEUS dodanou dodavatelem (přes tlačítko „...“).
  - Zatrhneme příslušný set, který hodláme obnovit (nabídne se nám pouze jeden).
  - Přejdeme na záložku „Options“, zatrhneme možnost „[x] Overwrite the existing database“ a zkontrolujeme, že se databázové soubory obnoví ve správné lokaci.
  - Zahájíme restore databáze stisknutím tlačítka „OK“.
3. Ověříme konfiguraci – viz oddíl 3.2.2.
4. Nastavíme oprávnění, které jsou požadovány dalšími komponentami CROSEUS – viz příslušné kapitoly „Potřebná oprávnění“ u jednotlivých komponent.



### 3.2.3.2 Upgrade

Upgrade databáze lze provést automaticky v rámci aktualizace webové aplikace CROSEUS, nebo v některých výjimečných případech manuálně (jedná se o speciální a běžně nepodporovanou metodu aktualizace – o dostupnosti této metody vždy informuje dodavatel).

#### 3.2.3.2.1 Upgrade (automaticky)

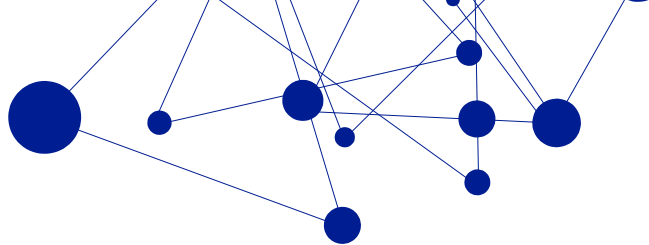
Viz popis aplikace Dynatech Installer – oddíl 3.8.3.

#### 3.2.3.2.2 Upgrade (manuálně)

1. Manuálně provedeme zálohu příslušné databáze CROSEUS.
2. Provedeme upgrade databáze aplikací předpřipravené sady SQL skriptů. Skripty dodává dodavatel v rámci nasazení. Menší sady skriptů (obvykle obsahující 1-4 soubory) aplikujeme ručně. Větší sady skriptů aplikujeme spuštěním jednoduché konzolové aplikace Dynatech DbUp, která je dodávána místo skriptů (a již je plně nakonfigurovaná pro provozní prostředí).

### 3.2.4 Minimální HW a SW nároky

- HW konfigurace databázového serveru:
  - ≤100 uživatelů: více jádrový 2GHz CPU, 8 GB RAM, 1 Gbit/s NIC
  - >100 uživatelů: více jádrový 2GHz CPU, 8 GB RAM, 10 Gbit/s NIC
- Databázový engine Microsoft SQL Server 2012, 2014, 2016 nebo 2017, edice Express a vyšší, včetně posledního dostupného service packu.



## 3.3 Aplikace Dynatech Signature Tool

### 3.3.1 Popis

Aplikace DST je nástroj určený pro uživatelské koncové stanice, na kterých bude probíhat podepisování PDF dokladů aplikace CROSEUS. Z technického pohledu je to registrovaná COM komponenta pro platformu Microsoft Windows, která umí vyhledat certifikát v osobním úložišti certifikátů aktuálně přihlášeného uživatele a tento použít k podepsání otisku PDF dokumentu, který získá od aplikace CROSEUS. K operaci podpisu využívá algoritmy z rodiny SHA-2.

Nástroj DST nemá žádné GUI. Informace o průběhu a výsledcích instalace/odinstalace vypisuje do standardního aplikačního logu operačního systému. Nástroj je dodáván ve formě instalačního MSI balíčku.

### 3.3.2 Konfigurace

Nástroj DST nenabízí žádné dodatečné konfigurační volby.

Během instalace dojde k registraci COM komponenty a URI handleru „croseus“ v registrech operačního systému. Konkrétně vzniknou nové klíče/větve:

- HKEY\_CLASSES\_ROOT\Dynatech.Foundation.Security.CmsSignerX509\
- HKEY\_CLASSES\_ROOT\CLSID\{[GUID\_komponenty\_vygenerovaný\_OS<sup>17</sup>]}\  
  • HKEY\_CLASSES\_ROOT\croseus\

Zprávy o výsledcích registrace/odregistrace vypisuje nástroj DST do standardního aplikačního logu operačního systému. Jako zdroj události zde uvádí hodnotu „DST“.

### 3.3.3 Instalační postupy

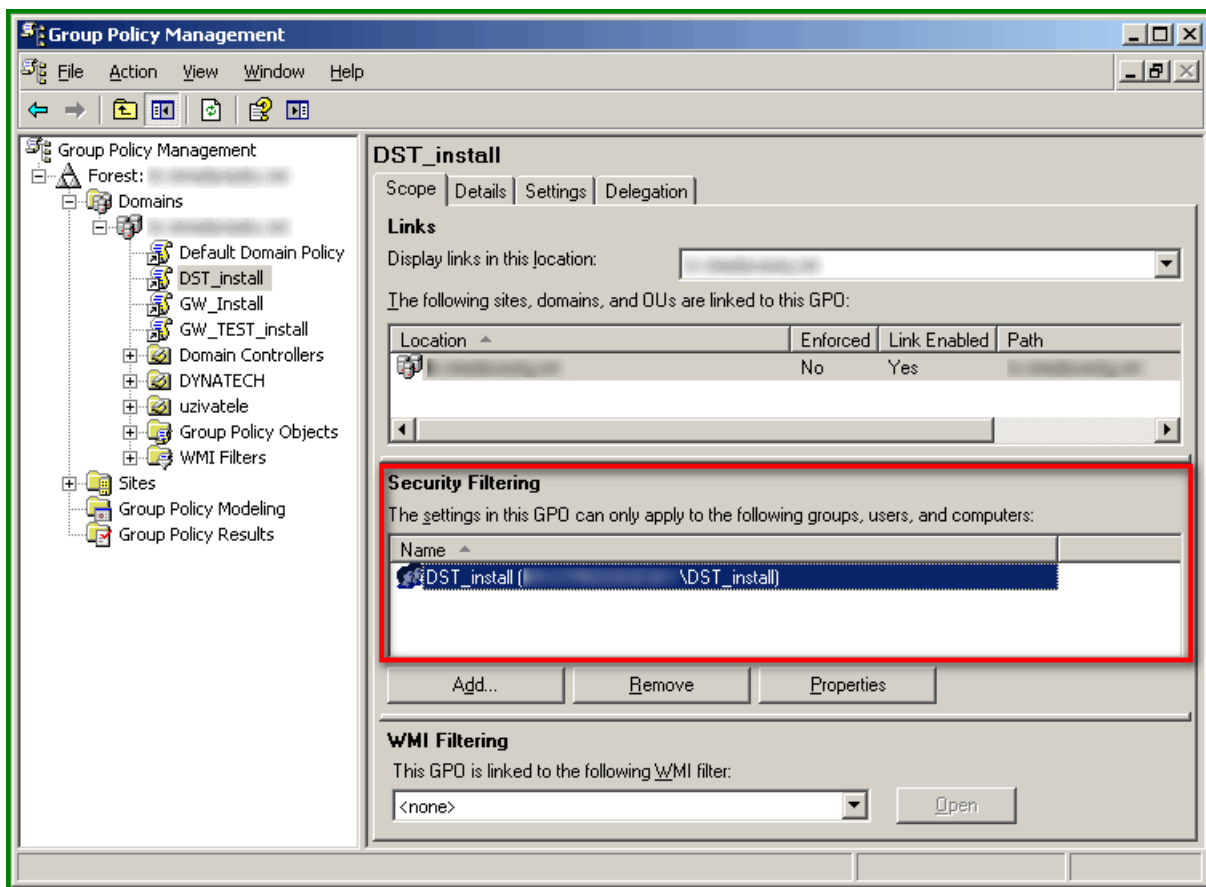
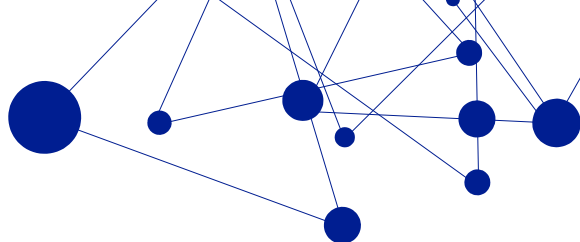
#### 3.3.3.1 Nasazení aplikace DST pomocí Active Directory

##### 3.3.3.1.1 První instalace

Pro plošné nasazení DST pomocí Active Directory (dále AD) je vhodné vytvořit samostatný Group Policy Object (dále GPO). Na tomto objektu je třeba nastavit vhodné „filtrování zabezpečení“ tak, aby se software dostal na požadovanou skupinu počítačů. Doporučeným postupem je skupinu počítačů sdružit v rámci jedné, k těmto účelům vytvořené, doménové skupiny.

---

<sup>17</sup> Při každé instalaci se může lišit. Správu GUIDů si řídí operační systém samostatně a aplikace DST do tohoto procesu nemůže nijak zasáhnout. Aktuálně použitý GUID lze ovšem vždy dohledat v klíči „HKEY\_CLASSES\_ROOT\Dynatech.Foundation.Security.CmsSignerX509\CLSID“.

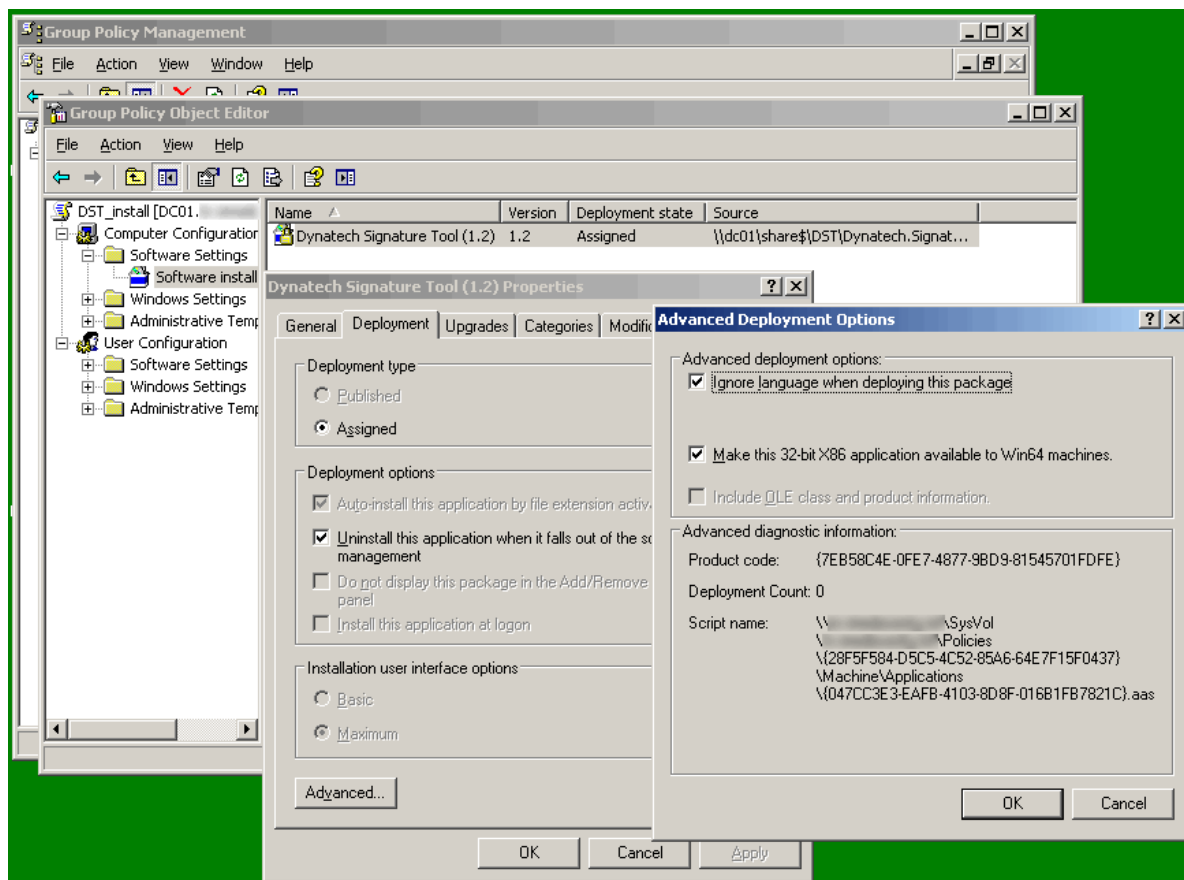
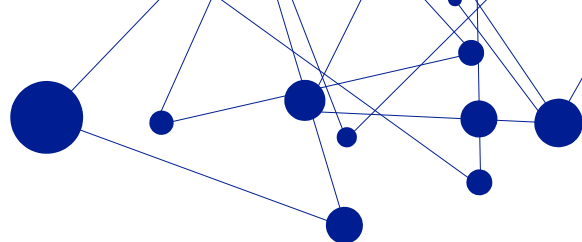


Obrázek 4 – GPO – filtrování zabezpečení

Po vytvoření GPO provedeme tyto kroky:

- 1) Přejdeme do vlastností politiky, do míst, kde můžeme provést vložení MSI balíčku aplikace DST (tj. do větve „Computer Configuration“ --> „Software Settings“ --> „Software Installation“)
- 2) Provedeme import balíčku:
  - a. „New...“ --> „Package“
  - b. Deployment typ: „(o) Advanced“
  - c. Přejdeme na záložku „Deployment“
  - d. Zaškrtneme „[x] Uninstall this application when ...“
  - e. Klikneme na tlačítko „Advanced...“
  - f. Zaškrtneme „[x] Ignore language when deploying this package“
  - g. „OK“
  - h. zbytek voleb ponecháme v defaultním nastavení
  - i. „OK“





Obrázek 5 – GPO – nastavení MSI balíčku

3) Aplikujeme GPO v rámci provozního prostředí.

### 3.3.3.1.2 Upgrade

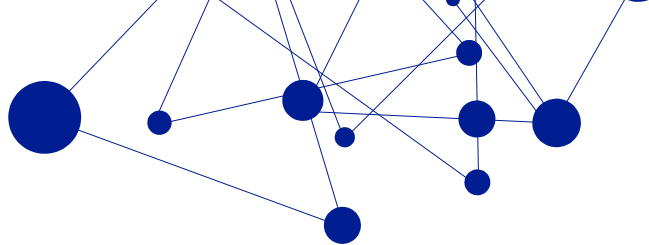
Upgrade balíčku na novou verzi probíhá nahrazením původního MSI balíčku v Active Directory novým balíčkem. U upgradu je velmi důležité myslet na to, že není možné nainstalovat nové MSI jako upgrade, ale je nezbytně nutné nejdříve starou verzi MSI z politiky odebrat, a při odebírání vynutit odinstalování balíčku ze všech počítačů (není nutné čekat na samotnou odinstalaci, jen je nutné odinstalaci vynutit politikou – volba „All Tasks“ --> Remove... --> „Immediately uninstall the software from users and computers“).

### 3.3.3.2 Manuální nasazení aplikace DST

Manuální nasazení aplikace DST probíhá jednoduše tak, že se dvojklikem inicializuje MSI balíček aplikace a projde se jednotlivými obrazovkami průvodce instalací.

Během instalace je možné zvolit místo uložení aplikace, zde ovšem doporučujeme ponechat defaultní hodnotu. V opačném případě nedojde po dokončení instalace k úspěšné registraci nové COM komponenty a bude třeba registraci provést dodatečně ručně – viz oddíl 3.3.3.3.

Při upgradu je nutné před samotnou instalací nové verze přes konzoli operačního systému „Přidat/odebrat programy“ vynutit odinstalaci staré verze.



### 3.3.3.3 Manuální registrace COM komponenty

Dodatečnou registraci aplikace DST jako COM komponenty lze provést spuštěním jednoduché řádkové CMD aplikace „register\_COM.cmd“ která je po instalaci produktu uložena přímo v kořenovém adresáři aplikace DST (defaultně „c:\Program Files\DYNA-TECH\Dynatech Signature Tool\“).

Spustí-li se aplikace „register\_COM.cmd“ s parametrem „/r“, nedojde k přímému zápisu do registrů, ale aplikace vygeneruje REG soubor, který uloží v kořenovém adresáři aplikace DST, a který lze později aplikovat do registrů manuálně.

### 3.3.4 Potřebná oprávnění

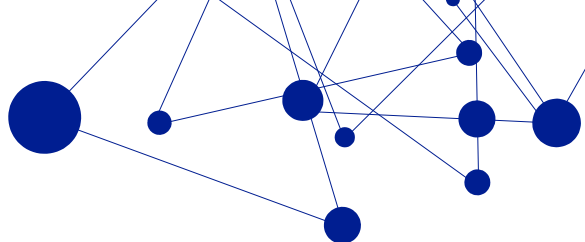
- a) Instalace aplikace DST musí být prováděna v kontextu a pod právy lokálního administrátora operačního systému.

### 3.3.5 Minimální HW a SW nároky

- Operační systém Microsoft Windows 7, 8.1 nebo 10
- Microsoft .NET Framework 4.5 až 4.7.2<sup>18</sup>
- V rámci lokálního profilu každého uživatele (respektive uživatelského účtu), který v aplikaci CROSEUS může provádět schvalování, musí být v úložišti osobních certifikátů účtu umístěn osobní X.509 certifikát s následujícími vlastnostmi:
  - Musí obsahovat privátní klíč.
  - Musí být použitelný pro podpisování, tj. např. v klíčových vlastnostech („key usage“) mít uveden příznak „Digital Signature“.
  - Certifikátu musí operační systém věřit (tj. musí být platný, důvěryhodný atd.).
  - Certifikát nesmí figurovat na revokačním listu certifikační autority, která jej vydala.<sup>19</sup>

<sup>18</sup> Je defaultní součástí některých operačních systémů Windows. Na další lze doinstalovat. Podrobnosti viz [http://msdn.microsoft.com/en-us/library/bb822049\(v=vs.110\).aspx](http://msdn.microsoft.com/en-us/library/bb822049(v=vs.110).aspx)

<sup>19</sup> Z tohoto důvodu je třeba vždy zajistit, aby aplikace měla přístup k revokačnímu listu dané certifikační autority. Pokud jej nemá, nedokáže 100% ověřit platnost certifikátu a při podpisu jej uživateli vůbec nenabídne k použití.



## 3.4 Certifikát softwarového vydavatele Dynatech

### 3.4.1 Popis

Certifikát softwarového vydavatele Dynatech (dále certifikát) umožňuje koncovým uživatelům aplikací z rodiny produktů CROSEUS provádět prostřednictvím aplikací i operace, které nějak manipulují s lokálními zdroji jejich koncových stanic. Typicky je třeba ke zpřístupnění následujících operací:

- Podepisování dokumentů
- Vkládání příloh

Certifikát není potřeba k diskovým operacím (např. otevření/uložení PDF souboru) ani k ovládání aplikace přes webové rozhraní.

Aktuální certifikát lze stáhnout ze stránek <https://pp.dynatech.cz/download/Certifikaty/>. Dodáván je ve formě samostatného souboru CER nebo instalačního MSI balíčku, který lze využít k hromadné distribuci např. v prostředí bez pokrytí Active Directory.

### 3.4.2 Konfigurace

Certifikát nelze dodatečně konfigurovat.

Během instalace certifikátu prostřednictvím MSI balíčku dojde také k související úpravě v registrech operačního systému (viz oddíl 3.1.4, bod c). Konkrétně se nastaví hodnota klíče „AllowElevatedTrustAppsInBrowser“ na „1“. Klíč se nachází v:

- „HKEY\_LOCAL\_MACHINE\Software\Microsoft\Silverlight“ na 32bit OS
- „HKEY\_LOCAL\_MACHINE\Software\Wow6432Node\Microsoft\Silverlight“ na 64bit OS

### 3.4.3 Instalační postupy

#### 3.4.3.1 Nasazení certifikátu Dynatech pomocí Active Directory (Windows 2008 a vyšší)

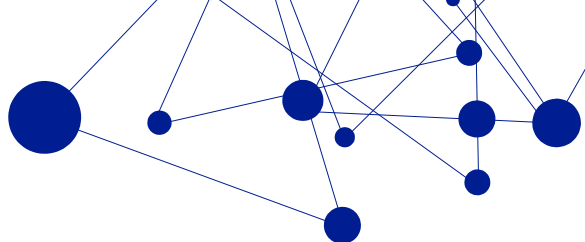
##### 3.4.3.1.1 První instalace

Pro plošné nasazení certifikátu prostřednictvím Active Directory (dále AD) lze využít v podstatě jakýkoliv nový nebo existující Group Policy Object (dále GPO). Na tomto objektu ovšem musíme nastavit vhodné „filtrování zabezpečení“ tak, aby se certifikát dostal k požadované skupině počítačů/uživatelů.

Po vytvoření GPO provedeme tyto kroky:

- 1) Přejdeme do vlastností politiky, do míst, kde můžeme provést vložení certifikátu (tj. do větve „Computer Configuration“ --> „Windows Settings“ --> „Security Settings“ --> „Public Key Policies“ --> „Trusted Publishers“).
- 2) Provedeme import certifikátu pomocí volby „Action“ --> „Import“ --> postupujeme dle instrukcí průvodce pro import certifikátů.
- 3) Aplikujeme GPO v rámci provozního prostředí.

##### 3.4.3.1.2 Upgrade



Upgrade certifikátu na novou verzi probíhá nahrazením původního certifikátu v Active Directory novým certifikátem. Postup je shodný jako v případě prvního nasazení. Původní certifikát je vhodné z politiky odebrat.

### 3.4.3.2 Nasazení certifikátu Dynatech pomocí Active Directory (Windows 2003)

#### 3.4.3.2.1 První instalace

Pro plošné nasazení certifikátu prostřednictvím Active Directory (dále AD) lze využít v podstatě jakýkoliv nový nebo existující Group Policy Object (dále GPO). Na tomto objektu ovšem musíme nastavit vhodné „filtrování zabezpečení“ tak, aby se certifikát dostal k požadované skupině počítačů/uživatelů.

Po vytvoření GPO provedeme tyto kroky:

- 1) Přejdeme do vlastností politiky, do míst, kde můžeme provést vložení certifikátu (tj. do větve „Computer Configuration“ --> „Windows Settings“ --> „Security Settings“ --> „Software Restriction Policies“).
- 2) Vytvoříme novou Software Restriction politiku, pokud dosud žádná neexistuje (klikneme pr. tl. myši nad „Software Restriction Policies“ --> „New Software Restriction Policies“).
- 3) Provedeme import certifikátu:
  - a. Přejdeme do „Additional Rules“
  - b. V panelu nástrojů zvolíme „Action“ --> „New Certificate Rule...“
  - c. Pomocí tlačítka „Browse...“ zvolíme cílový certifikát
  - d. Změníme vlastnost „Security level“ na hodnotu „Unrestricted“
  - e. Vše potvrdíme tlačítkem „OK“
- 4) Aplikujeme GPO v rámci provozního prostředí.

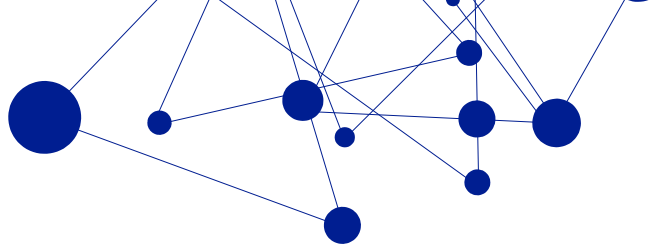
#### 3.4.3.2.2 Upgrade

Upgrade certifikátu na novou verzi probíhá nahrazením původního certifikátu v Active Directory novým certifikátem. Postup je shodný jako v případě prvního nasazení. Původní certifikát je vhodné z politiky odebrat.

### 3.4.3.3 Manuální nasazení certifikátu ve formě souboru CER

Manuální nasazení certifikátu probíhá následujícím způsobem:

- a. Na klientskou stanici si stáhneme soubor s certifikátem (CER)
- b. Dvojklikem jej otevřeme a klikneme na tlačítko „Install Certificate...“
- c. „Next“
- d. Zvolíme možnost „(o) Place all certificates in following store“
- e. „Browse...“
- f. Zvolíme adresář „Trusted Publishers“ (pokud bychom zvolili jiný, nebude řešení fungovat) a klikneme na „OK“
- g. „Next“



h. Vše potvrdíme tlačítkem „Finish“ a počkáme na dokončení instalace

Upgrade probíhá totožně.

#### **3.4.3.4 Manuální nasazení certifikátu ve formě MSI balíčku**

Manuální nasazení certifikátu přes instalační MSI balíček probíhá jednoduše tak, že tento dvojklikem inicializujeme a projdeme jednotlivými obrazovkami průvodce instalací.

Během instalace je možné zvolit místo uložení instalačních souborů certifikátu, zde ovšem doporučujeme ponechat defaultní hodnotu. V opačném případě nedojde po dokončení instalace k úspěšné registraci certifikátu a bude třeba registraci provést dodatečně ručně – postup viz oddíl 3.4.3.3.

Informace o úspěchu/neúspěchu registrace certifikátu se vypisuje do aplikačního logu operačního systému. Jako zdroj je uveden „DynCert“.

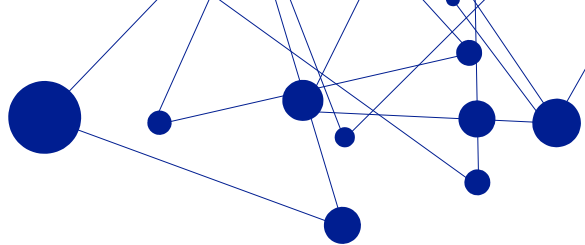
Při upgradu je vhodné před samotnou instalací nové verze přes konzoli operačního systému „Přidat/odebrat programy“ vynutit odinstalaci staré verze.

#### **3.4.4 Potřebná oprávnění**

- b) Instalace certifikátu ve formě CER souboru musí být prováděna v kontextu a pod právy lokálního uživatele operačního systému.
- c) Instalace certifikátu prostřednictvím MSI balíčku musí být prováděna v kontextu a pod právy lokálního administrátora operačního systému.

#### **3.4.5 Minimální HW a SW nároky**

- Operační systém Microsoft Windows 7, 8.1 nebo 10
- Operační systém musí důvěřovat certifikační autoritě VeriSign (<http://www.verisign.com/>)



## 3.5 Aplikace Dynatech Scheduler

### 3.5.1 Popis

Dynatech Scheduler je nástroj určený pro aplikační/webový server, na kterém je provozována serverová část aplikace CROSEUS. Z technického pohledu se jedná o konzolovou aplikaci pro platformu Microsoft Windows, která je ve formě EXE souboru začleněna k souborům webu aplikace CROSEUS. Jedná se o mnohem jednodušší obdobou defaultně instalované aplikace operačního systému Windows – Task Scheduler. Tj. nástroj dokáže vyvolat/provádět předem definované úlohy (z množiny možných variant) v předem definovaných časových intervalech. Jeho předností je mnohem užší vazba na celé řešení řídicí kontroly a možnost provádět operace „šitě na míru“, které by v běžném Task Scheduleru byly obtížně realizovatelné.

Pro potřeby aplikace CROSEUS umí Dynatech Scheduler vyvolat následující úlohy:

- **Aktualizovat subjekty vůči ARES** – Ověří aktuálnost dat všech subjektů v evidenci vůči ARES (provozuje ministerstvo financí ČR). Pokud nalezne rozdíl, data automaticky aktualizuje.
- **Ověření spolehlivosti plátce DPH** – Ověří u všech subjektů z aplikace CROSEUS zda jsou, nebo nejsou spolehlivými plátcí DPH dle vývěsky systému ARES ministerstva financí ČR.
- **Ověřit platnost osob v rolích** – Ověří u všech osob z aplikace CROSEUS zda jsou stále platné.
- **Přesunout archivované doklady do souborového systému** – Na základě nastavení datového úložiště provádí migraci dokladů z databáze do souborového systému, nebo naopak.
- **Údržba indexu v databázi** – Na základě používání aplikace CROSEUS dochází u většiny tabulek v databázi k vyšší fragmentaci indexů, což je nežádoucí. Tato úloha zajišťuje opravu formou rebuildu, či reorganizací indexů.
- **Zápis počtu dokladů dle stavů a typů ŘK k danému datu** – Vytváří statistiky o práci s doklady.

Nástroj nemá žádné samostatné GUI, konfiguraci úloh je nutné provádět z prostředí aplikace CROSEUS.

Pro podporu automatického spouštění úloh v naplánovaných časech je nutné nástroj propojit s aplikací Microsoft Task Scheduler<sup>20</sup> (detaily viz oddíl 3.5.2). Dynatech Scheduler nespouští úlohy přímo. Místo toho, ve chvíli kdy je zavolán Task Schedulerem, u každé úlohy nejdříve ověří, zda již uplynul definovaný interval od jejího posledního běhu. Pokud ano, úlohu spustí. Pokud ne, přeskočí ji a pokračuje další úlohou v pořadí.

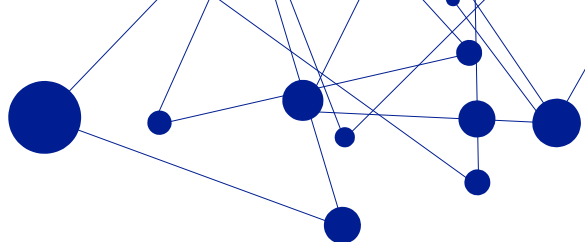
Informace o posledním průběhu jednotlivých událostí se zapisují do databáze CROSEUS. Viditelné jsou z prostředí aplikace CROSEUS. Aplikace také vytváří historický chybový log soubor v souborovém systému aplikačního serveru.

Skončí-li některá operace Dynatech Scheduleru chybou, odešle aplikace CROSEUS informační hlášení ve formě emailu všem osobám v roli „Správce integrací“.

### 3.5.2 Konfigurace

Hlavním účelem programu je spouštět definované úlohy – detaily k nastavení viz jednotlivé podkapitoly. Rozhraní pro konfiguraci úloh není součástí aplikace Dynatech Scheduler, ale součástí

<sup>20</sup> V česko-jazyčných operačních systémech se komponenta jmenuje „Plánovač úloh“.



aplikace CROSEUS (sekce „Nastavení“ -> „nastavení aplikace“ -> „nastavení časovače“). Všechny informace o úlohách jsou ukládány do databáze CROSEUS (viz oddíl 3.2), včetně detailů týkajících se jejich posledního běhu.

Dojde-li při spuštění úlohy k chybě, je tato informace navíc zapsána i do externího TXT souboru/logu, včetně přesného času kdy k incidentu došlo. Log je defaultně umístěn v kořenovém adresáři webové aplikace CROSEUS pod názvem „*error\_log-[datum].txt*“ (umístění i název souboru je možné měnit).

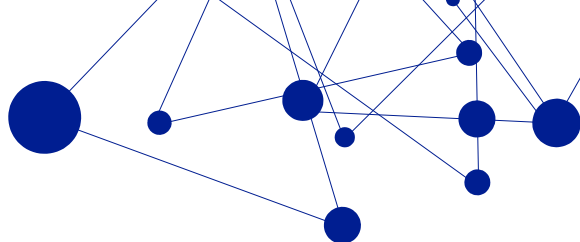
Některé obecné vlastnosti Dynatech Scheduleru jsou konfigurovatelné. Standardně aplikace využívá konfigurační miniaplikaci Dynatech Settings Manager a všechny konfigurační soubory aplikace CROSEUS (detaily viz část 3.1.1.1) s výjimkou souboru „Web.config“ v root adresáři (tj. konfigurace je v podstatě sdílená). Místo něj využívá vlastní konfigurační soubor „Dynatech.DFS.Scheduler.exe.config“. Soubor momentálně neobsahuje žádné volitelné parametry.

Dynatech Scheduler se nespouští samočinně. Bez dodatečné konfigurace se nikdy žádná úloha neprovede. Aby takový mechanismus fungoval, je třeba upravit běhové prostředí aplikačního serveru. Konkrétně musíme zajistit, aby byl soubor „Dynatech.DFS.Scheduler.exe“ spouštěn automaticky a v pravidelných intervalech. Proto aplikace počítá s využitím Microsoft Task Scheduleru<sup>21</sup>, konkrétně s vytvořením jedné nové úlohy s následujícími vlastnostmi:


- Záložka „General“
  - **Name:** Musíme uvést vhodné jméno, např. *Invoke Dynatech Scheduler*
  - **Security Options:**
    - U parametru „When running the task, use the following user account“ musíme nastavit vhodný servisní účet (viz oddíl 3.5.4)
    - Musíme zvolit hodnotu „(o) Run whether user is logged on or not“
- Záložka „Triggers“
  - Je vhodné vytvořit jedinou samostatnou aktivační událost společnou pro všechny Dynatech Scheduleru, který si přejeme automaticky spouštět. Obecně doporučené hodnoty:
    - **Begin the task:** „On a schedule“
    - **Settings:** Denně. Začátek [dnes] od 00:00:00, opakovat každý 1 den.
    - **Advanced settings:**
      - Pomocí parametru „Repeat task every“ je vhodné nastavit opakování úlohy na každých 15 minut<sup>22</sup>
      - Pomocí parametru „Stop task if it runs longer than“ je vhodné vynucovat zastavení úlohy, pokud poběží déle než 1 hodinu.

<sup>21</sup> Podrobný manuál k produktu Task Scheduler viz [http://msdn.microsoft.com/en-us/library/windows/desktop/aa383614\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa383614(v=vs.85).aspx)

<sup>22</sup> Obecně je vhodné nastavit interval kratší, než nejkratší z „period spouštění“ nastavených u jednotlivých úloh v aplikaci CROSEUS.



- Záložka „Actions“
  - Je vhodné vytvořit samostatnou akci pro každý Dynatech Scheduler, který si přejeme automaticky spouštět (typicky tedy jednu). Povinné hodnoty:
    - **Action:** Start a program
    - **Settings:** Do parametru „Program/script“ musíme nastavit úplnou cestu k souboru „Dynatech.DFS.Scheduler.exe“
- Ostatní vlastnosti nové úlohy doporučujeme ponechat v původním nastavení.

 **POZOR:** Jeden task v Task Scheduleru smí obsluhovat maximálně jednu aplikaci Dynatech Scheduler. Jinak bude docházet k neplánovaným chybám.

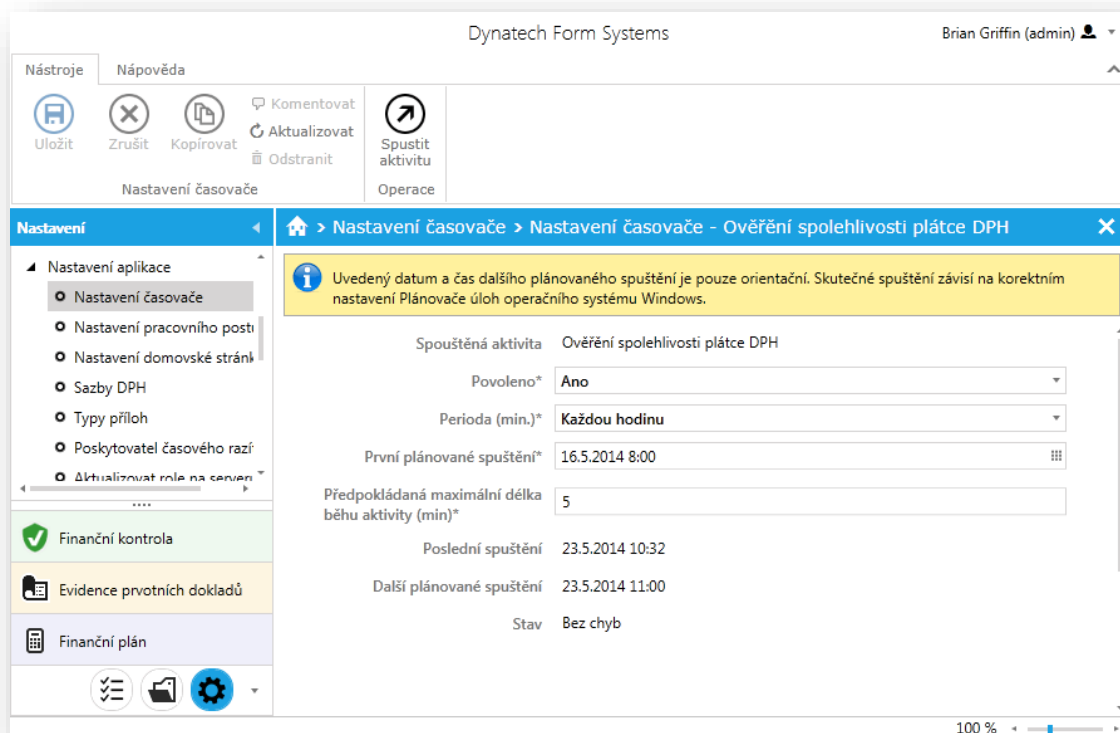
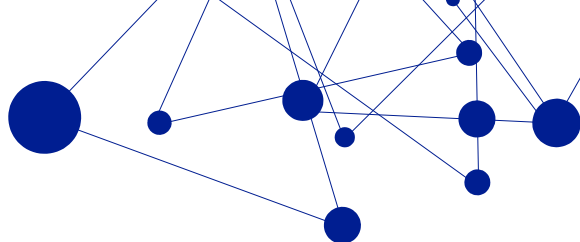
### 3.5.2.1 Společné vlastnosti všech úloh

Nastavení úlohy se skládá z parametrů:

Parametr	Význam
<b>Spouštěná aktivita</b>	Jedinečný název, pod kterým je úloha evidována v aplikaci CROSEUS. Atribut je neměnný.
<b>Povoleno</b>	Pokud je nastaveno na „Ano“, Dynatech Scheduler bude provádět automatické spouštění úlohy (řídí se přitom ostatními údaji). Pokud je nastaveno na „Ne“, úloha se automaticky provádět nebude ( <i>toto je defaultní nastavení u všech úloh</i> ). V obou případech lze úlohu spustit i ručně pomocí tlačítka „Spustit aktivitu“.
<b>Perioda</b>	Číslo udávající dobu, po jak dlouhých intervalech se má úloha automaticky spouštět. Může nabývat hodnot: „Nejnižší možná“, „Každou hodinu“, „Denně“, „Týdně“, „Měsíčně“, „Ročně“, nebo libovolnou číselnou hodnotu v minutách (povolený rozsah je 15-525600 minut). Atribut je povinný.
<b>První plánované spuštění</b>	Přesný datum a čas, od kterého se má zahájit počítání periody.
<b>Předpokládaná maximální délka běhu aktivity</b>	Hodnota v minutách, která udává, na jak dlouho se úloha zamkne v případě spuštění. Po dobu platnosti zámku není možné úlohu znovu spustit. Povolený rozsah je 5-1440 minut.
<b>Poslední spuštění</b>	Datum a čas posledního spuštění úlohy.
<b>Další plánované spuštění</b>	Datum a čas dalšího plánovaného spuštění úlohy. Jedná se o odhad. Přesný čas závisí na přesné chvíli spuštění Dynatech Scheduleru.
<b>Stav</b>	Pokud poslední běh úlohy skončí bez chyb, je zde uveden text „Bez chyb“. V opačném případě je zde uvedeno přesné chybové hlášení.

Vzorové nastavení viz následující obrázek.





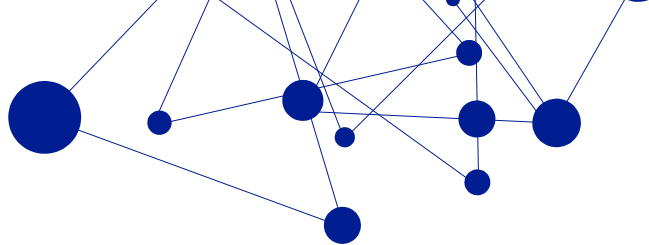
Obrázek 6 – Defaultní nastavení úlohy „Ověření spolehlivosti plátce DPH“

### 3.5.2.2 Úloha „Aktualizovat subjekty vůči ARES“

Doporučené nastavení úlohy:

Parametr	Doporučená hodnota
<b>Povoleno</b>	Ne Povolit jen v případě, že aktualizace po jednotlivých subjektech není dostačující.
<b>Perioda</b>	Denně (doporučeno spouštět mezi 18h-8h ranní)
<b>První plánované spuštění</b>	[Dnes]
<b>Předpokládaná maximální délka běhu aktivity</b>	60

Úloha má speciální nastavení týkající se využití lokální cache paměti. Více informací viz oddíl 3.1.2.1.1.



### 3.5.2.3 Úloha „Ověření spolehlivosti plátce DPH“

Doporučené nastavení úlohy:

Parametr	Doporučená hodnota
Povoleno	Ano
Perioda	Denně
První plánované spuštění	[Dnes]
Předpokládaná maximální délka běhu aktivity	10

### 3.5.2.4 Úloha „Ověřit platnost osob v rolích“

Doporučené nastavení úlohy:

Parametr	Doporučená hodnota
Povoleno	Ano
Perioda	Denně
První plánované spuštění	[Dnes]
Předpokládaná maximální délka běhu aktivity	10

### 3.5.2.5 Úloha „Přesunout archivované doklady do souborového systému“

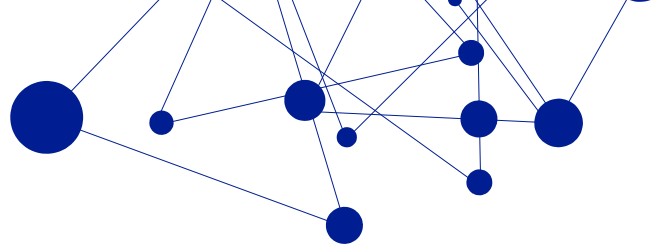
Doporučené nastavení úlohy:

Parametr	Doporučená hodnota
Povoleno	Ne Povolit jen v případě, že velikost přidružené databáze CROSEUS překročí 10 GB.
Perioda	Týdně (víkend)
První plánované spuštění	[Dnes]
Předpokládaná maximální délka běhu aktivity	60

### 3.5.2.6 Úloha „Údržba indexu v databázi“

Doporučené nastavení úlohy:

Parametr	Doporučená hodnota
Povoleno	Ano
Perioda	Týdně (víkend)
První plánované spuštění	[Dnes]
Předpokládaná maximální délka běhu aktivity	60



### 3.5.2.7 Úloha „Zápis počtu dokladů dle stavů a typů ŘK k danému datu“

Doporučené nastavení úlohy:

Parametr	Doporučená hodnota
Povoleno	Ano
Perioda	Denně (před půlnocí)
První plánované spuštění	[Dnes]
Předpokládaná maximální délka běhu aktivity	60

### 3.5.2.8 Úloha „Zkompaktnění příloh“

Doporučené nastavení úlohy:

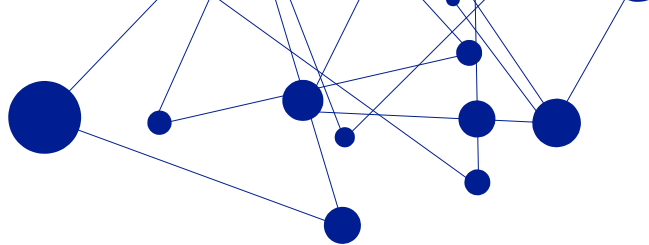
Parametr	Doporučená hodnota
Povoleno	Ano
Perioda	Denně (po půlnoci)
První plánované spuštění	1:00
Předpokládaná maximální délka běhu aktivity	60

## 3.5.3 Instalační postupy

Aplikace Dynatech Scheduler je dodávána jako součást webové aplikace CROSEUS. Instalace i upgrade probíhají současně s nasazením webu – postup viz oddíl 3.1.3. Při prvním nasazení je třeba navíc realizovat i úpravy popsané v části o konfiguraci (viz 3.5.2).

## 3.5.4 Potřebná oprávnění

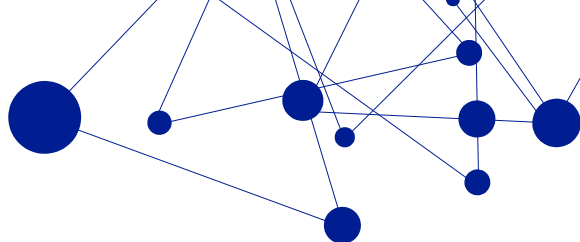
- a) Účet, pod kterým se spouští Dynatech Scheduler (a tedy i související úlohy Task Scheduleru), musí:
  - Vystupovat v rolích „log on as a service“ a „log on as a batch job“ v lokálních bezpečnostních politikách aplikačního serveru (jedná-li se o servisní účet).
  - Mít minimálně serverovou roli „public“ na SQL serveru, kde je provozována databáze CROSEUS.
  - Nad databází CROSEUS mít minimálně role: public a db\_slssystemaccount.
  - Nad adresářem, kde jsou umístěny soubory webové aplikace CROSEUS, mít práva: Read, Read&Execute a List Folder Content.
  - Nad adresářem, ve kterém se ukládají log soubory aplikace, mít práva: Read, Write, Modify, Read&Execute a List Folder Content.
  - Mít přístup k SMTP serveru za účelem odesílání informačních emailů
  - Mít přístup k internetu, konkrétně k adrese:
    - <http://adisrws.mfcr.cz:80> – využívá se k ověřování, zda subjekt užitý v procesu řídicí kontroly je spolehlivým plátcem DPH.



- (volitelně) Pokud je aktivována úloha „Přesunout archivované doklady do souborového systému“ (viz oddíl 3.5.2.4), mít nad adresářem, do kterého se PDF doklady přesouvají, práva: Read, Write, Read&Execute a List Folder Content.
  - **Doporučení:** Vzhledem k tomu, že všechny uvedené vlastnosti musí splňovat i účet, pod kterým běží aplikační pool webové aplikace CROSEUS, doporučujeme aplikaci Dynatech Scheduler spouštět pod stejným účtem.
- b) Konfigurace úloh v aplikaci CROSEUS může provádět pouze osoba v roli správce aplikace CROSEUS.

### 3.5.5 Minimální HW a SW nároky

- Operační systém Microsoft Windows Server 2008 a novější
- Microsoft .NET Framework 4.7.1 a vyšší
- Webová aplikace CROSEUS (viz oddíl 3.1) – Dynatech Scheduler je její defaultní součástí.
- Databáze CROSEUS (viz oddíl 3.2) – nemusí být umístěna lokálně, stačí, když k ní aplikace bude mít přístup. Je sdílená s komponentou CROSEUS.



## 3.6 Integrace s CROSEUS Identity Management

### 3.6.1 Popis

Aplikaci CROSEUS je možné integrovat s aplikací „CROSEUS Identity Management“ (dále CIM). Připojením k CIM je umožněno jednotné přihlašování ke všem produktům rodiny CROSEUS.

### 3.6.2 Konfigurace

Integraci mezi aplikacemi CROSEUS a CIM je nutné nakonfigurovat. To lze provést ručně, nebo pomocí průvodce.

Konfigurace integrace ze strany CROSEUS se provádí z prostředí „Dynatech Settings Manager – Nastavení aplikace“ (viz oddíl 3.1.2.1.1), sekce „Dynatech Auth Provider“ (viz 3.6.2.1). Konfigurace integrace ze strany CIM je popsána v technické dokumentaci řešení CIM.

#### 3.6.2.1 Nastavení „Dynatech Auth Provider“

Nastavení v Dynatech Settings Manageru se skládá z parametrů:

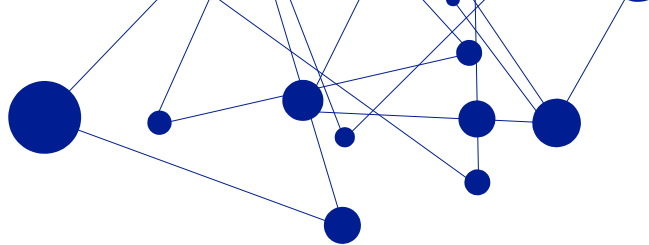
Položka	Význam
CIM - Url	URL k poskytovateli identit (CIM). Pokud není vyplněno, aplikace není s CIM integrována. Výchozí hodnota je prázdná. Doporučovaný postup připojení k CIM: zadat adresu k CIM a kliknout na „Registrovat“. Po zadání údajů pro CIM budou hodnoty vyplněny na obou stranách.
Identifikátor aplikace	Identifikátor aplikace vůči poskytovateli identit.
Klíč aplikace	Sdílené tajemství s poskytovatelem identit.

Vzorové nastavení viz následující obrázek:

### Dynatech Auth Provider

Položka	Hodnota	Popis
CIM - Url	<input style="width: 100%;" type="text"/> <a href="#" style="color: #007bff; text-decoration: none;">Registrovat</a>	URL k poskytovateli identit (CIM). Pokud není vyplněno, aplikace není s CIM integrována. Výchozí hodnota je prázdná. Doporučovaný postup připojení k CIM: zadat adresu k CIM a kliknout na Registrovat. Po zadání údajů pro CIM budou hodnoty vyplněny na obou stranách.
Identifikátor aplikace	<input style="width: 100%;" type="text"/>	Identifikátor aplikace vůči poskytovateli identit
Klíč aplikace	<input style="width: 100%;" type="text"/>	Sdílené tajemství s poskytovatelem identit

Obrázek 7 – Vzorové nastavení Dynatech Auth Provider na straně CROSEUS



### 3.6.3 Zprovoznění integrace

#### 3.6.3.1 Zprovoznění integrace pomocí průvodce

1. Otevřeme „Dynatech Settings Manager – Nastavení aplikace“ aplikace CROSEUS a přejdeme k sekci „Dynatech Auth Provider“, viz 3.6.2.1.
2. Do pole „CIM – Url“ vložíme URL k aplikaci CIM a klikneme na odkaz „Registrovat“
3. Aplikace nás požádá o přihlášení do nastavení aplikace CIM.
4. Po přihlášení se konfigurační údaje automaticky předvyplní, vzor viz následující obrázek:

**Připojit systém k poskytování identit**

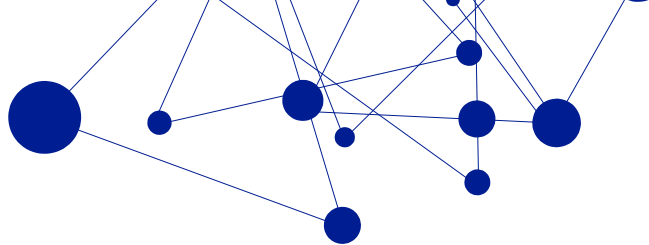
Název	CROSEUS - SM (iis8.office.dynatech.cz
Identifikátor aplikace	https__iis8.office.dynatech.cz_ORK_ x
Klíč aplikace	vzxfUpt?Rg
Url	https://iis8.office.dynatech.cz/ORK/devsr
Zpětná url	https://iis8.office.dynatech.cz/ORK/devsr

Obrázek 8 – Příklad automaticky předvyplněné konfigurace během registrace integrace CROSEUS-CIM

5. Hodnoty parametrů „Název“, „Identifikátor aplikace“ i „Klíč aplikace“ můžeme libovolně změnit.
6. Po stisknutí tlačítka „Nastavit“ dojde k uložení konfigurace do obou aplikací (CIM i CROSEUS), a integrace se tímto zprovozní.

#### 3.6.3.2 Zprovoznění integrace ručně

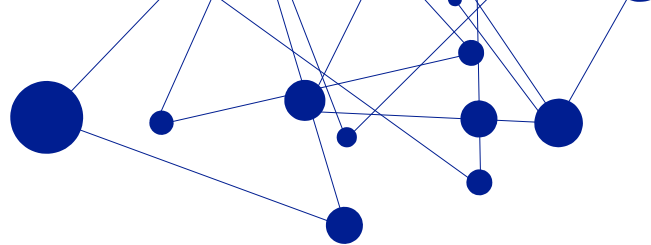
1. Předpokládá se, že osoba v roli správce CIM provedla nastavení v CIM ručně (viz technická dokumentace systému CIM) a předala potřebné hodnoty pro ruční vyplnění osobě, která provádí konfiguraci aplikace CROSEUS (tj. správci aplikace CROSEUS).
2. Otevřeme „Dynatech Settings Manager – Nastavení aplikace“ aplikace CROSEUS a přejdeme k sekci „Dynatech Auth Provider“, viz 3.6.2.1.



3. Získané údaje od správce CIM vložíme do jednotlivých polí a klikneme na „Uložit“. Integrace se tímto zprovozní.

### 3.6.3.3 Zrušení integrace

1. Otevřeme „Dynatech Settings Manager – Nastavení aplikace“ aplikace CROSEUS a přejdeme k sekci „Dynatech Auth Provider“, viz 3.6.2.1.
2. Z dané sekce vymažeme ze všech polí všechny hodnoty a změnu uložíme prostřednictvím tlačítka „Uložit“.
3. V CIM odstraníme související integrovaný systém (viz technická dokumentace systému CIM).



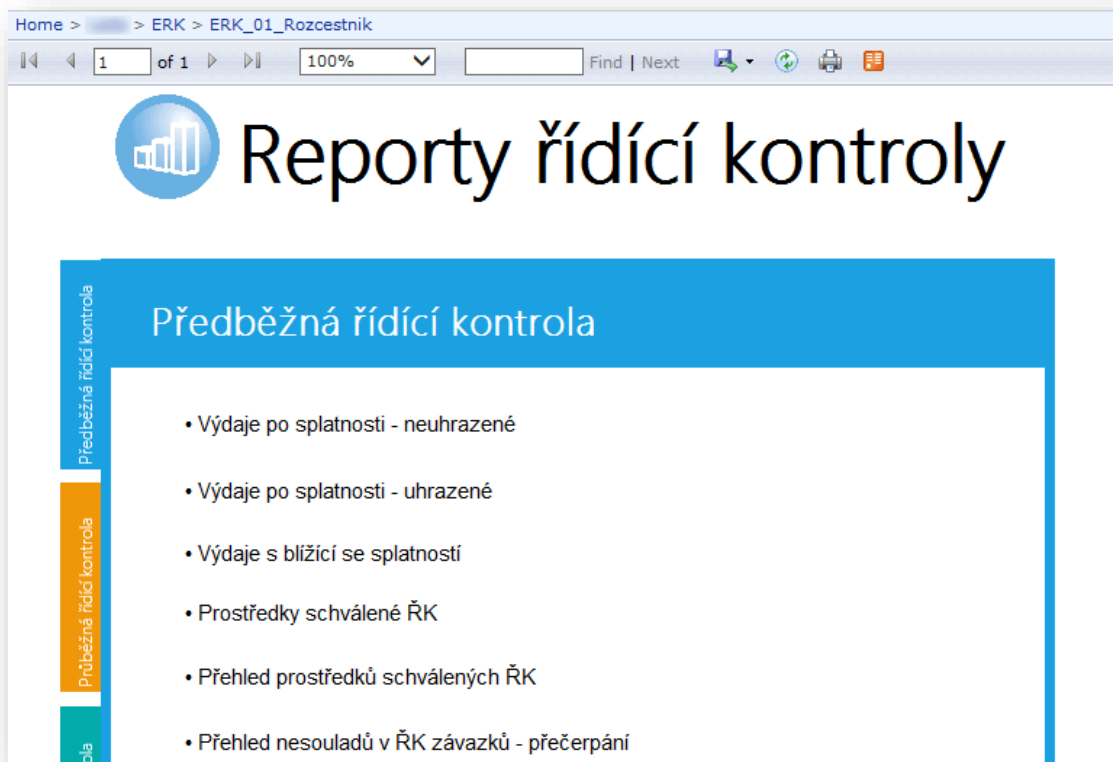
## 3.7 Reporty CROSEUS

### 3.7.1 Popis

Reporty pro modul elektronické řídicí kontroly umožňují detailnější analýzu dat z databáze CROSEUS a jejich hlavním účelem je podpora manažerských a rozhodovacích procesů. Je to volitelná komponenta, která může (ale nemusí) být nasazena na stejném databázovém serveru, jako je umístěna databáze CROSEUS.

**ERK\_01\_Rozcestník** je hlavním reportem celé sady. Obsahuje rozcestník, z kterého uživatel může otevřít libovolný další report. Reporty jsou přehledně rozděleny dle oblastí, kterých se týkají. Seznam základních oblastí:

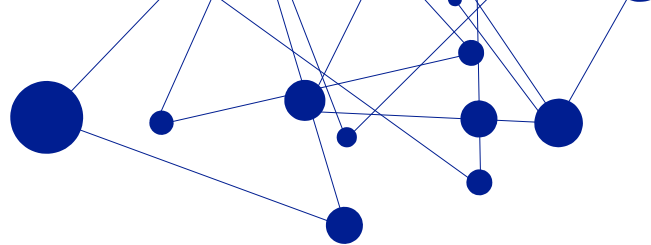
- Předběžná řídicí kontrola
- Průběžná řídicí kontrola
- Následná řídicí kontrola
- Archiv
- Správa



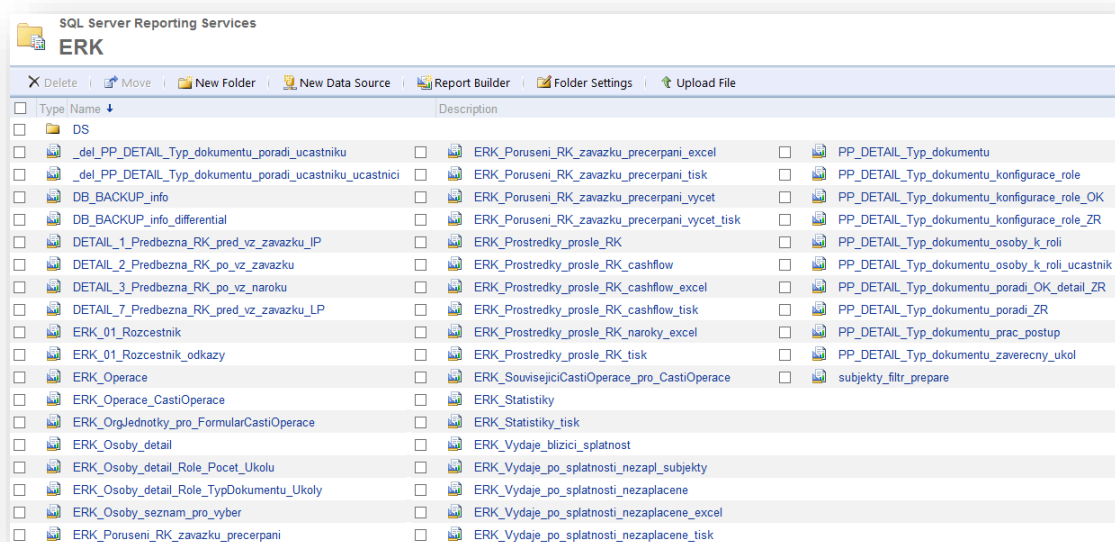
Obrázek 9 – Podoba reportu ERK\_01\_Rozcestník

Mimo hlavní report jsou součástí řešení i další reporty, které nejsou uživateli přímo viditelné. Slouží jako subreporty, což znamená, že se zobrazují jako dílčí část nějakého dalšího reportu.





Úplný seznam reportů pro zobrazení dat týkajících elektronické řídi kontroly je na následujícím obrázku.

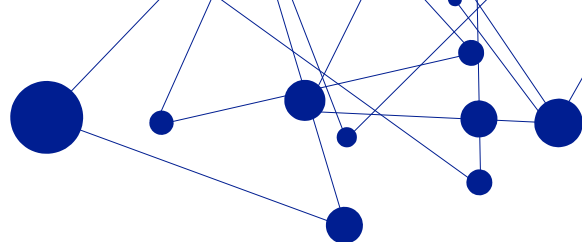


Obrázek 10 – Úplný přehled reportů CROSEUS

### 3.7.2 Konfigurace

Konfigurace reportů se provádí ve webovém rozhraní SQL Reporting Services (jedná se o běžnou součást tohoto produktu firmy Microsoft). Zde je možné zobrazit a upravovat vlastnosti každého jednotlivého reportu. U všech reportů lze zachovat většinu vlastností tak, jak je server automaticky nastaví během jejich nahrávání na server (děje se v rámci nasazení, viz příslušný oddíl). Výjimku tvoří následující konfigurace:

- U reportů, které nejsou považovány za výchozí, doporučujeme nastavit parametr „[x] Hide in list view“ na záložce „General“ v nastavení reportu.
- Každý report musí být nakonfigurovaný tak, aby pracoval s datovým zdrojem, který odkazuje na databázi CROSEUS. Ideální variantou je vytvořit sdílený datový zdroj, který je pak pro všechny reporty společný (usnadňuje to jakoukoliv pozdější rekonfiguraci).
- Datový zdroj musí pracovat s databází CROSEUS. Přístup datového zdroje k databázi ovšem může být řešen libovolně. Nejčastější varianty jsou:
  - Přístup prostřednictvím servisního SQL účtu. Vzor nastavení viz následující obrázek (text uvedený v hranatých závorkách nahraďte platnými hodnotami, dle stavu ve Vašem provozním prostředí):



Name: [jméno\_zdroje]

Description: [ ]

Hide in tile view

Enable this data source

Data source type: Microsoft SQL Server

Connection string: data source=[SQL\_instance];initial catalog=[název\_databáze\_ÉRK]

Connect using:

Credentials supplied by the user running the report

Display the following text to prompt user for a user name and password:

[Type or enter a user name and password to access the data source]

Use as Windows credentials when connecting to the data source

Credentials stored securely in the report server

User name: [jméno\_SQL\_úctu]

Password: [ ]

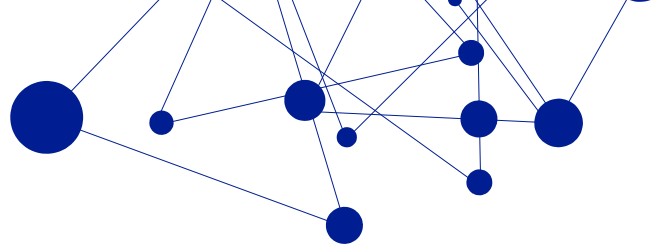
Use as Windows credentials when connecting to the data source

Impersonate the authenticated user after a connection has been made

Windows integrated security

Credentials are not required

- Přístup prostřednictvím servisního Windows účtu. Vzor nastavení viz následující obrázek (text uvedený v hranatých závorkách nahraďte platnými hodnotami, dle stavu ve Vašem provozním prostředí):



Name: [jméno\_zdroje]

Description: [ ]

Hide in tile view

Enable this data source

Data source type: Microsoft SQL Server

Connection string: data source=[SQL\_instance];initial catalog=[název\_databáze\_ĚRK]

Connect using:

Credentials supplied by the user running the report

Display the following text to prompt user for a user name and password:

[Type or enter a user name and password to access the data source]

Use as Windows credentials when connecting to the data source

Credentials stored securely in the report server

User name: [doména]\[jméno\_účtu]

Password: [.....]

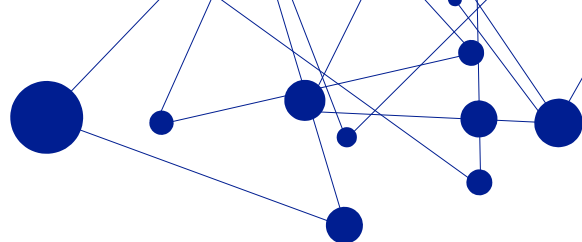
Use as Windows credentials when connecting to the data source

Impersonate the authenticated user after a connection has been made

Windows integrated security

Credentials are not required

- Přístup přímo pod identitou přihlášeného uživatele. Vzor nastavení viz následující obrázek (text uvedený v hranatých závorkách nahraďte platnými hodnotami, dle stavu ve Vašem provozním prostředí):



Name: [jméno\_zdroje]

Description: [ ]

Hide in tile view

Enable this data source

Data source type: Microsoft SQL Server

Connection string: data source=[SQL\_instance];initial catalog=[název\_databáze\_ÉRK]

Connect using:

Credentials supplied by the user running the report

Display the following text to prompt user for a user name and password:

Type or enter a user name and password to access the data source

Use as Windows credentials when connecting to the data source

Credentials stored securely in the report server

User name: [ ]

Password: [ ]

Use as Windows credentials when connecting to the data source

Impersonate the authenticated user after a connection has been made

Windows integrated security

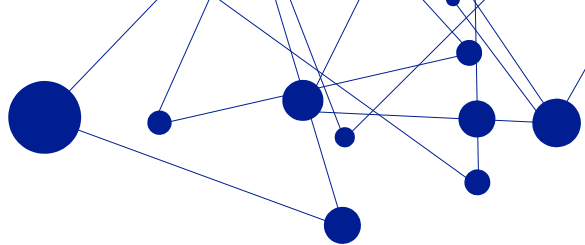
Credentials are not required

### 3.7.3 Instalační postupy

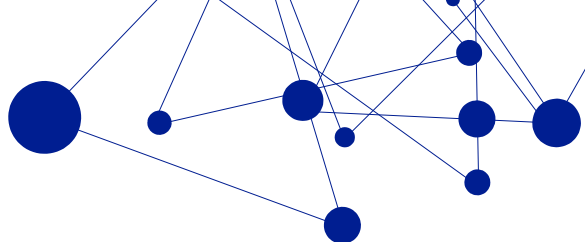
#### 3.7.3.1 Manuální nasazení reportů CROSEUS

##### 3.7.3.1.1 První nasazení

1. Přejdeme na server, kde je provozována služba SQL Reporting Services a otevřeme webové rozhraní (Report Manager) pro tuto službu.
2. Na domovské stránce rozhraní definujeme nové uživatelské role:
  - a. Přejdeme na odkaz „Site Settings“ (pravý horní roh obrazovky) → „Security“.
  - b. Prostřednictvím tlačítka „New role Assignment“ přidáme roli „[x] System User“ všem uživatelům, kteří s reporty mají pracovat. Roli uživatelům můžeme přidělit i nepřímo – stačí je zařadit do doménové skupiny, a teprve této skupině roli přidělit (toto je doporučený postup).



3. Nahrajeme reporty na report server:
  - a. Na domovské stránce webového rozhraní vytvoříme novou složku.
  - b. Vstoupíme do ní a pomocí tlačítka "Upload File" postupně naimportujeme všechny dodané RDL soubory.
4. Definujeme sdílený datový zdroj:
  - a. Ve složce s naimportovanými reporty vytvoříme novou složku pro datové zdroje.
  - b. Přejdeme do této složky a klikneme na tlačítko „New Data Source“. Načte se formulář, na kterém vyplníme údaje – viz oddíl 3.7.2.
  - c. Formulář odešleme tlačítkem „Apply“.
5. Na nový datový zdroj navážeme jednotlivé reporty:
  - a. Vrátime se do složky s naimportovanými reporty.
  - b. Klikneme na tlačítko "Show Details" → u reportů se objeví sloupeček „edit“. Pro každý report zvlášť provedeme:
    - i. Klikneme na ikonku „edit“
    - ii. V levém panelu snadného spuštění přejdeme na „Data Sources“.
    - iii. Vybereme možnost „(o) A shared data source“ a klikneme na „Browse“.
    - iv. Zvolíme datový zdroj vytvořený v rámci bodu č.4.
    - v. Klikneme na „Apply“.
6. (Volitelně) Skryjeme reporty, které pro běžné uživatele nejsou podstatné:
  - a. Vrátime se do složky s naimportovanými reporty.
  - b. Klikneme na tlačítko "Show Details" → u reportů se objeví sloupeček „edit“. Pro každý skrývaný report zvlášť provedeme:
    - i. Klikneme na ikonku „edit“
    - ii. V levém panelu snadného spuštění přejdeme na „General“.
    - iii. Zaškrtneme pole „[x] Hide in list view“.
    - iv. Klikneme na „Apply“.
7. Udělíme práva nad cílovými databázemi systémovému účtu nebo přímo koncovým uživatelům – viz příslušný oddíl o potřebných oprávněních.
8. Udělíme práva nad reporty příslušným uživatelům:
  - a. Vrátime se do složky s naimportovanými reporty.
  - b. Prostřednictvím tlačítka „New role Assignment“ udělíme uživatelům, kteří s reporty mají pracovat, definovaná práva (viz oddíl 3.7.4). Práva uživatelům můžeme přidělit i nepřímo – stačí je zařadit do doménové skupiny, a teprve této skupině práva přidělit (toto je doporučený postup). Alternativně je možné pro všechny uživatele zřídit jediný přístupový účet, který budou sdílet, a pak je nutné udělit práva pouze tomuto účtu.



### 3.7.3.1.2 Upgrade

1. Přejdeme na server, kde je provozována služba SQL Reporting Services a otevřeme webové rozhraní pro tuto službu.
2. Přejdeme do adresáře, ve kterém jsou nasazeny reporty, které se chytáme aktualizovat.
3. Postupně jednotlivé reporty aktualizujeme podle následujícího postupu:
  - a. Klikneme na tlačítko „Upload file“ → „Browse...“ → zvolíme novou verzi aktualizovaného reportu a zatrhneme nastavení „[x] Overwrite item if it exists“.
  - b. Změnu potvrdíme tlačítkem „OK“.
  - c. Zkontrolujeme, že se u reportu zachovala vazba na datový zdroj:
    - i. Klikneme na tlačítko „Show Details“.
    - ii. Klikneme na „Edit“ u daného reportu.
    - iii. V levém panelu snadného spuštění přejdeme na „Data Sources“.
    - iv. Pokud se zdroj nezachoval, zatrhneme nastavení „(o) A shared data source“ → „Browse...“ → zvolíme validní datový zdroj a klikneme na „Apply“.

### 3.7.3.2 Automatické nasazení reportů CROSEUS

#### 3.7.3.2.1 První nasazení

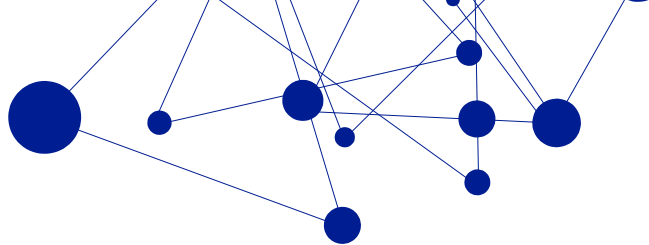
Jak je vidět z předchozího oddílu, reportů CROSEUS je velké množství. Naše firma proto dodává k nasazení této sady reportů i speciální řešení ve formě několika skriptů, které uživatelům systému umožní celé nasazení automatizovat. Řešení sestává z komponent:

- **VBS skript „GetAllReportFiles“** – skript v úvodní části obsahuje sadu konfigurovatelných proměnných (před prvním užitím je třeba je ověřit/upravit). V závislosti na konkrétních hodnotách pak skript po svém spuštění provede automatické nasazení RDL souborů z definovaného adresáře na Report server, vytvoří nový sdílený datový zdroj a tento zdroj připojí ke všem reportům. Ke svému běhu vyžaduje skript „PublishStandardReports.rss“.
- **RSS skript „PublishStandardReports“** – Obsahuje logiku pro komunikaci s Report serverem. Samostatně se nespouští.
- **SQL skript „Hide\_subreports\_CROSEUS“** – Po nasazení reportů na Report server je vhodné skrýt všechny ty, které jsou považovány za subreporty. Skript „Hide\_subreports\_CROSEUS“ tuto problematiku řeší. Aplikuje se do ReportServer databáze a před použitím je nutné v něm správně specifikovat všechny cesty k reportům CROSEUS (jedná se o cesty na úrovni webového rozhraní Report Serveru. Každá cesta je relativní a začíná na úrovni „Home“ adresáře).

### 3.7.4 Potřebná oprávnění

Potřebná oprávnění závisí na konkrétním nastavení datového zdroje jednotlivých reportů (viz oddíl 3.7.2). Zde jsou popsány dvě nejčastější varianty:

- a) **Varianta A** – přístup prostřednictvím servisního SQL nebo Windows účtu:
  - a. Systémový účet musí mít:
    - i. Serverovou roli „public“ na SQL serveru, kde je provozována databáze CROSEUS.

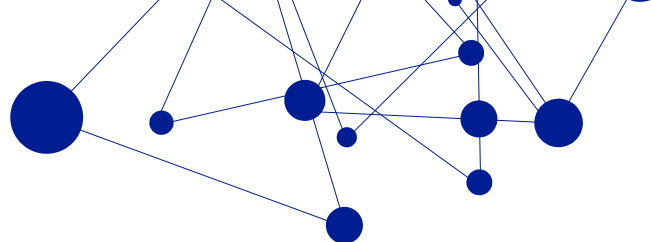


- ii. Nad databází CROSEUS role: db\_rsuser a public.
- b) **Varianta B** – přístup přímo pod identitou přihlášeného uživatele:
  - a. Každý oprávněný uživatel (pokud nejsou uživatelé sdruženi do jedné Windows bezpečnostní skupiny, v tom případě stačí udělit práva této skupině) musí mít:
    - i. Serverovou roli „public“ na SQL serveru, kde je provozována databáze CROSEUS.
    - ii. Nad databází CROSEUS role: db\_rsuser a public.

Dále musí mít každý uživatel roli „Browser“ na webovém rozhraní SQL Reporting Services na adresáři, ve kterém jsou reporty CROSEUS umístěny i na reportech samotných.

### 3.7.5 Minimální HW a SW nároky

- Microsoft SQL Server Reporting Services 2012 a vyšší (komponenta je součástí Microsoft SQL Serveru od edice „Express with Advanced Tools“)
- Databáze CROSEUS používaná aplikací CROSEUS (viz oddíl 3.2) – nemusí být umístěna lokálně, stačí, když k ní reporty budou mít přístup.

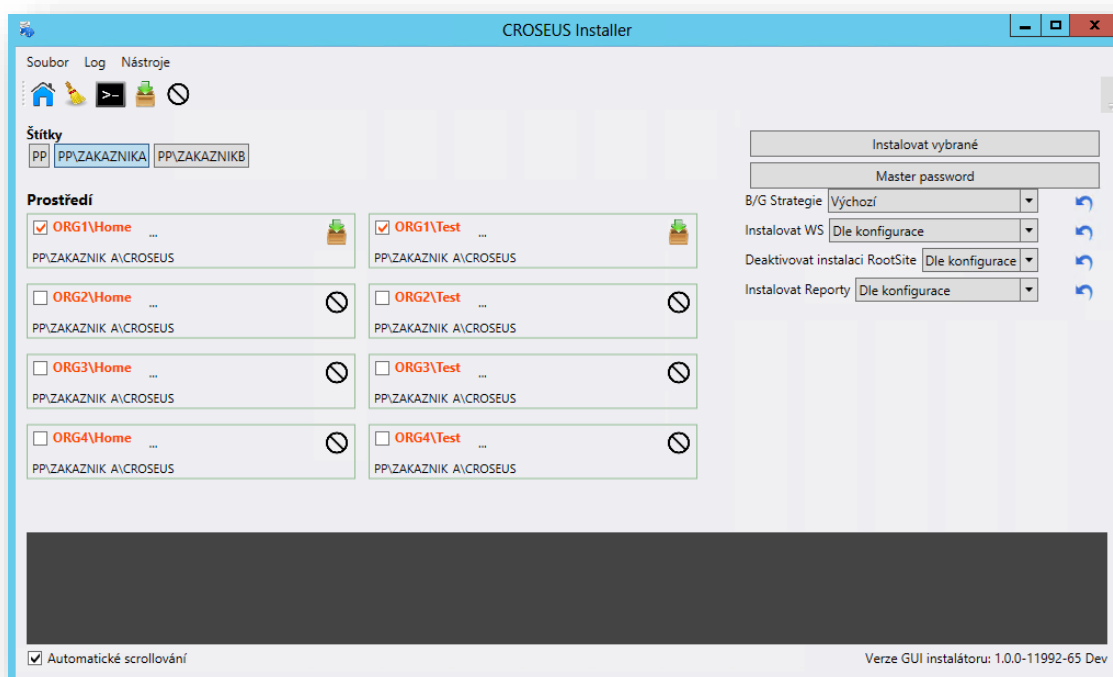


## 3.8 Instalátor DYNATECH Installer

### 3.8.1 Popis

Dynatech Installer (dále DI) je aplikace sloužící k bezproblémové a co nejvíce samočinné instalaci i aktualizaci všech produktů systému CROSEUS. Hlavní vlastnosti:

- Každou instalaci/aktualizaci lze spouštět opakovaně
- Průběh instalace/aktualizace je logován.
- Systém CROSEUS lze aktualizovat po částech, nebo v jediném celku
- DI umí nasadit/aktualizovat více instancí systému CROSEUS najednou.



Obrázek 11 – Základní dashboard instalátoru DYNATECH Installer

DI je dodáván jako sada nástrojů. Hlavní proces se spouští pomocí EXE aplikace „installer\_gui“.

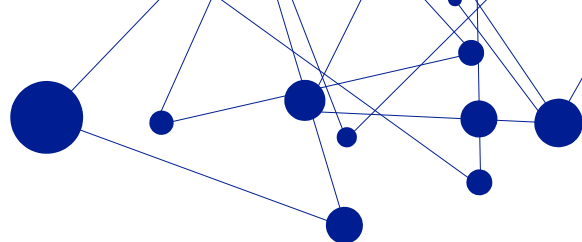
### 3.8.2 Konfigurace

Hlavní funkčnost produktu DI je založená na speciálních šablonách ve formátu XML (v dokument jsou dále označovány jako „DI šablony“). Každá DI šablona obsahuje sadu informací poplatných pro jednu konkrétní nasazovanou instanci systému CROSEUS.

V rámci konfigurace DI je možné:

1. Volit, které DI šablony mají být při instalaci použity, tj. na jaká prostředí má být nasazeno.
2. Upravovat údaje uvedené v jednotlivých DI šablonách, tj. lokálně upravovat parametry každé jednotlivé instalace (a tyto změny trvale uložit).

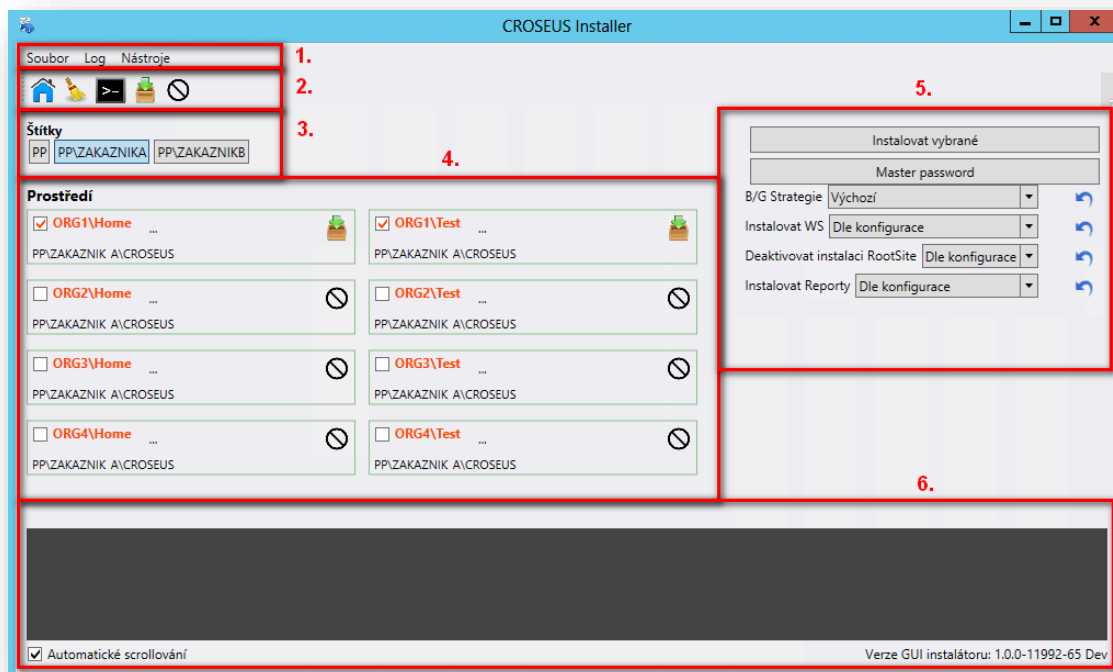




3. Hromadně přepisovat některé parametry z DI šablon, pokud v nich uvedená strategie instalace neodpovídá aktuálnímu záměru, tj. globálně nahrazovat parametry instalace ve všech instalacích najednou (pouze pro jednorázové využití).

Pro snadnou orientaci a editace je DI vybaveno grafickým rozhraním. To je spolu s popisem dostupných konfiguračních parametrů rozebráno v následujících podkapitolách.

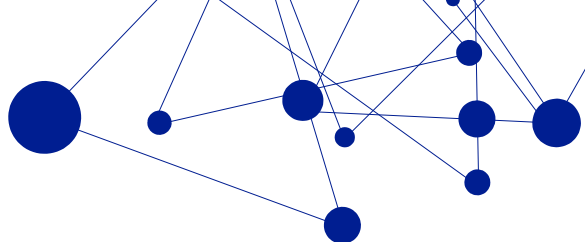
### 3.8.2.1 Grafické rozhraní DYNATECH Installeru



Obrázek 12 – Základní GUI instalátoru DYNATECH Installer

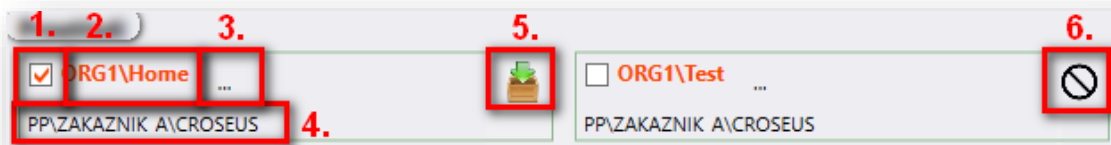
GUI DI se skládá z několika oblastí (viz obrázek výše):

1. **Nabídková lišta** – Obsahuje méně používané funkce produktu (Otevřít adresář aktualizací balíčku, Spustit příkazový řádek a další)
2. **Panel nástrojů** – Obsahuje základní a nejčastěji používané funkce produktu:
  - a. Tlačítko „Dashboard“ – návrat na základní obrazovku DI
  - b. Tlačítko „Smazat log“ – vymaže text zobrazený v oblasti „Okno logu“
  - c. Tlačítko „Příkazový řádek“ – spustí příkazový řádek operačního systému
  - d. Tlačítko „Vybrat zobrazené“ – automaticky označí všechny aktuálně zobrazená prostředí z oblasti „Prostředí“ k instalaci.
  - e. Tlačítko „Zrušit výběr“ – opak funkce tlačítka „Vybrat zobrazené“
3. **Štítky** – Soustava tlačítek, která umožňují filtrovat, která prostředí jsou aktuálně zobrazena v oblasti „Prostředí“. Seznam dostupných štítků se mění dynamicky na základě struktury uložení DI šablon v souborovém systému.



4. **Prostředí** – Zobrazení jednotlivých DI šablon. U každé šablony je k dispozici několik funkcí. Detaily viz samostatná podkapitola 3.8.2.1.1.
5. **Globální konfigurace** – Úkony, nebo nastavení, které se mají realizovat u všech zvolených DI šablon. Zvolená operace se provede okamžitě.
  - a. *Tlačítko „Instalovat vybrané“* – Zahájí instalace systému CROSEUS na zvolené prostředí. Instalace probíhá sériově. Pokud dojde k chybě, je uživatel vyzván k rozhodnutí, zda celý proces instalace přerušit, či pokračovat dalším prostředím.
  - b. *Tlačítko „Master password“* – Vyvolá dialog, kam lze zadat heslo, kterým se automaticky zašifrují všechna hesla, která jsou uvedena v jednotlivých DI šablonách. Po jeho zadání, se objeví tlačítka „Změnit“ a „Odstranit“, která umožňují heslo upravit, nebo všechny zašifrované údaje permanentně dešifrovat.
  - c. *Volba „B/G strategie“* – Hromadně nastaví způsob uplatňování B/G strategie pro instalované/aktualizované systémy CROSEUS.
  - d. *Volba „Instalovat WS“* – Hromadně nastaví, zda v rámci instalace/aktualizace systémů CROSEUS instalovat i CROSEUS API (viz oddíl 3.1.1.2)
  - e. *Volba „Deaktivovat instalaci RootSite“* – Hromadně nastaví, zda v rámci instalace/aktualizace systémů CROSEUS vytvářet i strukturu nadřazeného IIS webu. Původní web, existuje-li, je během operace smazán.
  - f. *Volba „Instalovat reporty“* – Hromadně nastaví, zda v rámci instalace/aktualizace systémů CROSEUS instalovat i reporty CROSEUS (viz oddíl 3.7)
6. **Okno logu** – podrobný výpis všech provedených operací včetně výsledku (i chyb).

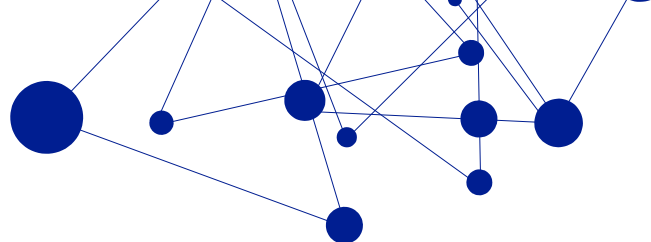
### 3.8.2.1.1 Prostředí



Obrázek 13 – Detail oblasti „Prostředí“

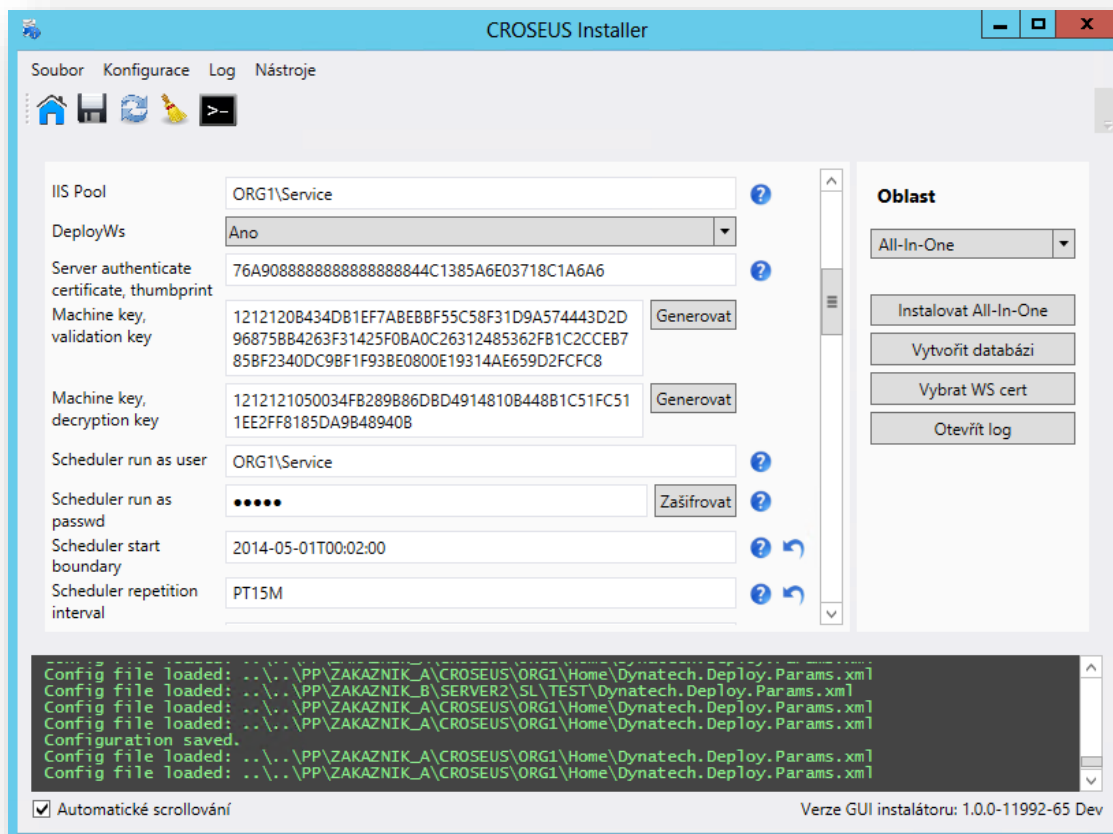
Oblast „Prostředí“ zobrazuje jednotlivé načtené DI šablony formou dlaždic. Každá dlaždice disponuje samostatnými ovládacími prvky (viz obrázek výše):

1. **Volba instalace** – pokud je zatrhnuto, dané prostředí bude začleněno do instalačního/aktualizačního procesu. Pokud ne, instalace se na daném prostředí neprovádí.
2. **Identifikátor DI šablony** – Druhá část cesty v souborovém systému k místu, kde je šablona uložena (napojuje se na údaj „Cesta k DI šabloně“, viz níže).
3. **Tlačítko „...“** – přechod ke konfiguraci dané DI šablony. Detaily viz oddíl 3.8.2.2.
4. **Cesta k DI šabloně** – první část cesty v souborovém systému k místu, kde je šablona uložena (vychází se z umístění „Installer\_gui.exe“ souboru).
5. **Indikátor instalace (varianta A)** – Pokud je „Volba instalace“ zatrhnuta, má tlačítko podobu balíčku. Po kliknutí se objeví instalační log.



6. Indikátor instalace (varianta B) – Vzhled tlačítka, pokud „Volba instalace“ zatrhnuta není.

### 3.8.2.2 DI šablona

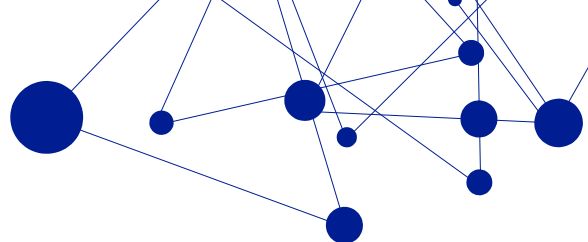


Obrázek 14 – detail konfigurace šablony DI z prostředí DI

Každá DI šablona je samostatný XML soubor s názvem „Dynatech.Deploy.Params.xml“. Aby se s ní dalo pracovat, musí být šablona umístěna v domovském adresáři DI (může však být zanořena do libovolného podadresáře).

K zobrazení konfigurace zvolené šablony DI se dostaneme po kliknutí na tlačítko „...“ (viz 3.8.2.1.1). Přes grafické rozhraní DI lze měnit a následně uložit řadu parametrů. Aktuální seznam včetně detailního popisu viz samostatný dokument „DYNATECH\_CROSEUS\_tech-nicka\_dokumentace\_Priloha\_A“.

Přes zobrazení konfigurace zvolené šablony DI lze rovněž provést pouze částečnou instalaci/-aktualizaci – detaily k tomuto režimu viz sekce 3.8.3.2.



### 3.8.3 Instalační postupy

#### 3.8.3.1 Instalace aplikace DYNATECH Installer

Aplikaci DI není nutné nijak instalovat. Jedná se o přenosnou EXE aplikaci.

#### 3.8.3.2 All-In-One instalace systému CROSEUS z prostředí DI

##### 3.8.3.2.1 První nasazení

1. Nainstalujeme prerekvizity pro běh produktu DI, viz 3.8.5.
2. Spustíme DI pomocí `installer_gui.exe`
3. V oblasti „Štítky“:
  - a. Kliknutím vybereme jeden, nebo více štítků, které označují námi instalované systémy CROSEUS.
4. V oblasti „Prostředí“:
  - a. Zatrhneme šablony DI, dle kterých chceme systém CROSEUS nainstalovat.
  - b. (volitelně) Přes tlačítko „...“ překontrolujeme a případně upravíme vlastnosti jednotlivých DI šablon.
  - c. (volitelně) Změny uložíme pomocí tlačítka „Uložit konfigurace“ z panelu nástrojů.
5. V oblasti „Globální konfigurace“:
  - a. Zadáme „Master password“, je-li v DI šablonách použito.
  - b. (volitelně) Upravíme nastavení parametrů „B/G strategie“, „Instalovat WS“, „Deaktivovat instalaci RootSite“ a „Instalovat reporty“ do námi požadovaných hodnot.
  - c. Spustíme instalaci pomocí tlačítka „Instalovat vybrané“.
6. Počkáme na dokončení instalace a dle informací z oblasti „Okno logu“ ověříme výsledek.

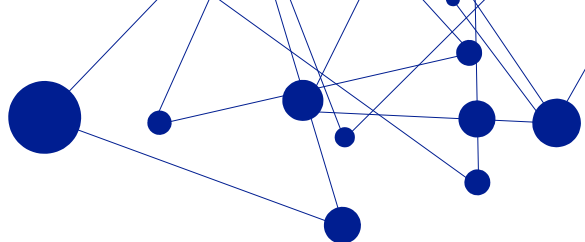
##### 3.8.3.2.2 Upgrade

Shodný s postupem pro první instalaci – viz 3.8.3.2.1. Bod č.1 se vynechává.

#### 3.8.3.3 Částečná instalace systému CROSEUS z prostředí DI – web

##### 3.8.3.3.1 První nasazení

1. Nainstalujeme prerekvizity pro běh produktu DI, mimo část určenou pro databázový server, viz 3.8.5.
2. Spustíme DI pomocí `installer_gui.exe`
3. V oblasti „Štítky“ kliknutím vybereme jeden, nebo více štítků, které označují námi instalovaný systém CROSEUS.
4. V oblasti „Globální konfigurace“:
  - a. Zadáme „Master password“, je-li v DI šablonách použito.
5. V oblasti „Prostředí“ zatrhneme právě jednu DI šablonu.
  - a. Přes tlačítko „...“ přejdeme na detail zvolené šablony.



- b. V oblasti „Oblast“ zvolíme „IIS“.
  - c. (volitelně) překontrolujeme a případně upravíme vlastnosti šablony.
  - d. (volitelně) Změny uložíme pomocí tlačítka „Uložit konfigurace“ z panelu nástrojů.
  - e. V oblasti „Oblast“ klikneme na tlačítko „Instalovat IIS“.
6. Počkáme na dokončení instalace a dle informací z oblasti „Okno logu“ ověříme výsledek.

### 3.8.3.3.2 Upgrade

Shodný s postupem pro první instalaci – viz 3.8.3.3.1. Bod č.1 se vynechává.

## 3.8.3.4 Částečná instalace systému CROSEUS z prostředí DI – databáze a reporty

### 3.8.3.4.1 První nasazení

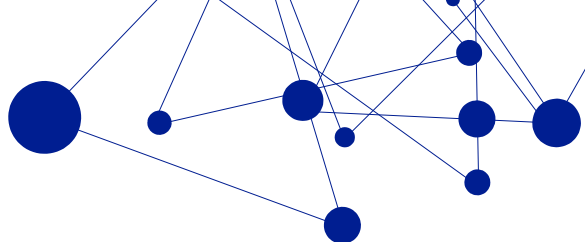
1. Nainstalujeme prerekvizity pro běh produktu DI, mimo část určenou pro aplikační/IIS server, viz 3.8.5.
2. Spustíme DI pomocí `installer_gui.exe`
3. V oblasti „Štítky“ kliknutím vybereme jeden, nebo více štítků, které označují námi instalovaný systém CROSEUS.
4. V oblasti „Globální konfigurace“:
  - a. Zadáme „Master password“, je-li v DI šablonách použito.
5. V oblasti „Prostředí“ zatrhneme právě jednu DI šablonu.
  - a. Přes tlačítko „...“ přejdeme na detail zvolené šablony.
  - b. V oblasti „Oblast“ zvolíme „DB“.
  - c. (volitelně) překontrolujeme a případně upravíme vlastnosti šablony.
  - d. (volitelně) Změny uložíme pomocí tlačítka „Uložit konfigurace“ z panelu nástrojů.
  - e. V oblasti „Oblast“ zvolíme „Reports“.
  - f. (volitelně) překontrolujeme a případně upravíme vlastnosti šablony.
  - g. (volitelně) Změny uložíme pomocí tlačítka „Uložit konfigurace“ z panelu nástrojů.
  - h. V oblasti „Oblast“ klikneme na tlačítko „Instalovat DB / Report“.
6. Počkáme na dokončení instalace a dle informací z oblasti „Okno logu“ ověříme výsledek.

### 3.8.3.4.2 Upgrade

Shodný s postupem pro první instalaci – viz 3.8.3.4.1. Bod č.1 se vynechává.

## 3.8.4 Potřebná oprávnění

- a) Uživatel, který spouští instalaci, musí mít práva:
  - a. Lokální administrátor na cílovém IIS serveru – pro část provádějící nasazení a úpravy v IIS a Windows Task Scheduler.
  - b. Sysadmin v cílové databázové instanci – pro část řešící aktualizaci databáze CROSEUS a nasazení reportů CROSEUS.



### 3.8.5 Minimální HW a SW nároky

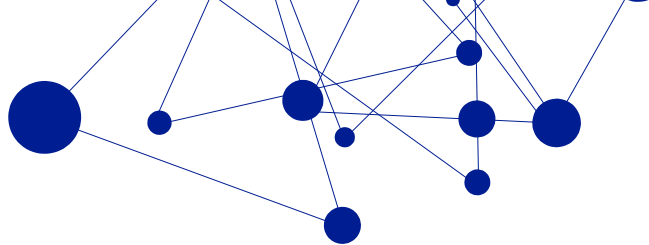
- Microsoft .NET Framework 3.5 SP1 a zároveň 4.7.1 nebo vyšší
- Web Deploy framework verze 3.0
  - <https://www.microsoft.com/cs-cz/download/details.aspx?id=30436>
- Dle instalovaných komponent všechny prerekvizity pro dané komponenty – viz jednotlivé kapitoly a oddíly s názvem „Minimální HW a SW nároky“ uvedené v tomto dokumentu.
- Na databázovém/MS SQL serveru:
  - Otevřený UDP port 5355 [network discovery (LLMNR-UDP-In)], ve směru IN
- Na aplikačním/IIS serveru:



Místo manuální instalace níže uvedených prerekvizit lze na aplikačním serveru využít i speciální instalátor „DYNATECH WebDeploy 3.5 All-In-One Installer“, který je součástí každého aktualizacího balíčku.<sup>23</sup>

- Web Deploy verze 3.5
  - <http://www.iis.net/downloads/microsoft/web-deploy>
  - Nainstalovat dle dokumentace <http://www.iis.net/learn/install/installing-publishing-technologies/installing-and-configuring-web-deploy-on-iis-80-or-later>, oddíl „Using the web deploy installer to install web deploy“.
- Požadavky na role a rysy operačního systému (tj. co musí být nainstalováno) – CMD příkazy:
  - `dism /online /enable-feature /featurename:IIS-WebServerRole`
  - `dism /online /enable-feature /featurename:IIS-WebServerManagementTools`
  - `dism /online /enable-feature /featurename:IIS-ManagementService`
- Povolené klíče v registrech operačního systému – CMD příkazy:
  - `Reg Add HKLM\Software\Microsoft\WebManagement\Server /V EnableRemoteManagement /T REG_DWORD /D 1`
  - `Reg Add HKLM\Software\Microsoft\WebManagement\Server /V WindowsAuthenticationEnabled /T REG_DWORD /D 1`
- Spuštěná služba operačního systému „Web Management Service“ (alias „wmsvc“) nastavená v režimu spouštění „Automaticky“.
- Explicitně povolené použití NTLM autentizace vůči prostředí IIS
  - Viz [https://technet.microsoft.com/en-us/library/dd722796\(v=WS.10\).aspx](https://technet.microsoft.com/en-us/library/dd722796(v=WS.10).aspx), oddíl 7.
- Otevřený TCP port 8172 [web management service (HTTP Traffic-In)], ve směru IN

<sup>23</sup> V aktualizacím balíčku je vždy umístěn v cestě  
„\CROSEUS\Tools\WebDeployInstaller\WebDeployInstaller.exe“.



## 4 Zálohování

Aplikace CROSEUS pracuje s daty. Ta jsou pořizována uživateli. Nejcennějším obsahem jsou doklady, tzv. auditní stopy a informace o schvalovacích procesech, které ještě nebyly dokončeny. Všechno je uloženo v databázi CROSEUS, vyjma PDF dokladů, které mohou být volitelně uloženy i externě v souborovém systému. Každý zálohovací mechanismus by měl hlavně:

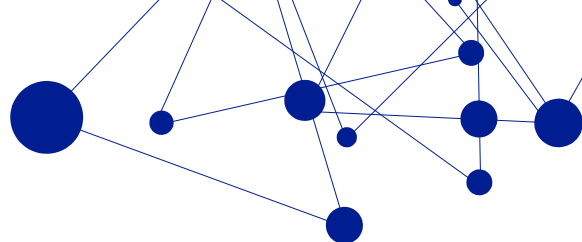
- Zajistit ochranu dat před ztrátou/poškozením
- Umožnit obnovu dat, pokud ke ztrátě nebo poškození dojde
- Zajistit dlouhodobou archivaci dat

Druhotně lze vzít v potaz i další hlediska:

- Rychlost obnovy celé služby v případě kritického selhání software/hardware
- Ochrana záloh před zcizením/neoprávněným užitím
- Velikost záloh, respektive požadavky na kapacitu úložného prostoru
- Požadavky na obsluhu

Obecně lze konstatovat, že pokud nemusíte řešit problém vysoké dostupnosti, postačí, budete-li doporučeným způsobem zálohovat databázi CROSEUS + všechny PDF doklady uložené v externím úložišti (jsou-li takové) + zajistíte-li dlouhodobou archivaci všech komponent, které jste obdrželi v rámci prvního i následujících nasazení systému CROSEUS.

Zálohy je vhodné uchovávat mimo vlastní databázové/aplikační servery, na kterých jsou provozovány jednotlivé komponenty systému CROSEUS.



## 4.1 Obecná doporučení pro zálohování databáze CROSEUS

Velikost organizace	Počet nových záznamů	Doporučený způsob zálohování	Maximální ztráta dat
Do 10 osob	0-10 denně	<ul style="list-style-type: none"> <li>• záloha transakčního logu               <ul style="list-style-type: none"> <li>○ pondělí – pátek, 1x denně (12:00)</li> </ul> </li> <li>• rozdílová záloha               <ul style="list-style-type: none"> <li>○ pondělí – sobota, 1x denně (noc)</li> </ul> </li> <li>• plná záloha               <ul style="list-style-type: none"> <li>○ 1x týdně (neděle)</li> </ul> </li> </ul>	8h práce
Do 50 osob	10-20 denně	<ul style="list-style-type: none"> <li>• záloha transakčního logu               <ul style="list-style-type: none"> <li>○ pondělí – pátek, 2x denně (12:00, 16:00)</li> </ul> </li> <li>• rozdílová záloha               <ul style="list-style-type: none"> <li>○ pondělí – sobota, 1x denně (noc)</li> </ul> </li> <li>• plná záloha               <ul style="list-style-type: none"> <li>○ 1x týdně (neděle)</li> </ul> </li> </ul>	4h práce
Do 100 osob	30-50 denně	<ul style="list-style-type: none"> <li>• záloha transakčního logu               <ul style="list-style-type: none"> <li>○ 1x každé 2h</li> </ul> </li> <li>• rozdílová záloha               <ul style="list-style-type: none"> <li>○ 1x denně (12:00)</li> </ul> </li> <li>• plná záloha               <ul style="list-style-type: none"> <li>○ 1x denně (noc)</li> </ul> </li> </ul>	2h práce
Nad 100 osob	>50 denně	<ul style="list-style-type: none"> <li>• záloha transakčního logu               <ul style="list-style-type: none"> <li>○ 1x každou 1h</li> </ul> </li> <li>• rozdílová záloha               <ul style="list-style-type: none"> <li>○ 2x denně (12:00, 16:00)</li> </ul> </li> <li>• plná záloha               <ul style="list-style-type: none"> <li>○ 1x denně (noc)</li> </ul> </li> </ul>	1h práce

## 4.2 Zálohování externího datového uložení PDF dokladů

Pokud je jako datové uložení pro PDF doklady zvolen souborový systém, je nutné provádět zálohu obsahu tohoto uložení ve stejné době jako zálohování databáze = tedy i se stejnou četností.

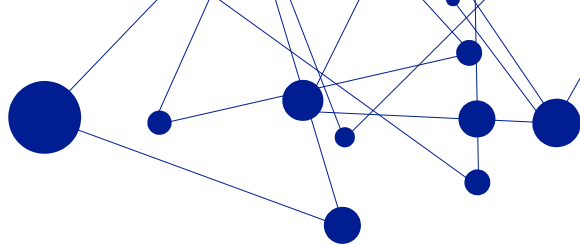
K zálohování lze využít vestavěných komponent operačních systémů Windows, např. Windows Backup<sup>24</sup>, NT Backup<sup>25</sup>, nebo WAdmin<sup>26</sup>. A samozřejmě i jiné nástroje od jiných certifikovaných výrobců.

<sup>24</sup> Viz <http://windows.microsoft.com/cs-cz/windows/back-up-files#1TC=windows-7>

<sup>25</sup> Viz <https://technet.microsoft.com/en-us/library/cc754423.aspx>

<sup>26</sup> Viz <https://technet.microsoft.com/en-us/library/cc742083.aspx>





### 4.3 Archivace záloh

Některé plné zálohy (minimálně však alespoň jednu za každý rok života systému), je vhodné skladovat/uchovávat dlouhodobě. Co přesně znamená „dlouhodobě“? To defacto záleží na typu dokladů, se kterými uživatelé v systému CROSEUS pracují. Délku minimálního (a někdy i maximálního) archivování dat totiž ve většině případů určuje zákon České Republiky.

Obecně lze říct, že doklad o provedené řídicí kontrole se uchovává po stejnou dobu, jako doklad, ke kterému se vztahuje (např. faktura, smlouva). Lhůty uchovávání těchto dokladů stanoví např. zákon č. 234/2004 Sb., o dani z přidané hodnoty, zákon č. 563/1991 Sb., o účetnictví, zákon č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení, nařízení Rady (ES) 1083/2006, Spisový a skartační řád dané organizace atd. – Např. u faktur s DPH je to 10 let, u mzdových dokladů 30 let, u EU projektů 20 let atd.<sup>27</sup>

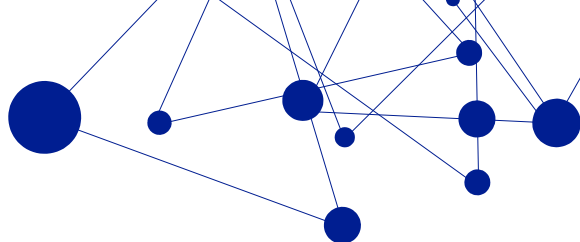
### 4.4 Optimalizační varianty

Velikost záloh lze značně snížit, bere-li zálohovací mechanismus v potaz pro danou organizaci obvyklé chování uživatelů systému – např. jejich běžnou pracovní dobu. Typicky je možné dle pracovní doby definovat zálohování transakčního logu a rozdílové zálohování např. jen na časové období pondělí-pátek, každý den od 7:00 do 19:00 apod.

Proces zálohování dat z externího úložiště je rovněž možné optimalizovat tak, aby se znovu zálohovaly vždy jen ty soubory, které se změnilly nebo přibýly od poslední plné zálohy.

---

<sup>27</sup> Přesnou dobu si prosím vždy ověřte v aktuálním znění zákona. Nařízené lhůty se mohou časem měnit.



## 5 Související dokumentace

Název	Popis	Odkaz na dokument
Technická dokumentace DYNATECH Správa Přístupů (CIM)		
Technická dokumentace DYNATECH CROSEUS – Příloha A		