DC Concept a.s.
Vídeňská 125
619 00 BRNO
Česká republika / Czech republic
Tel. +420 547125145
Fax +420 547125146
Email: info@dcconcept.cz

www.dcconcept.cz

Přístupová práva QI

Kontakt :

DC Concept a.s.
Vídeňská 125, 619 00 Brno, Tel:+420 547125145, Fax:+420 54712546
Dolní 71, 796 01 Prostějov,
http://www.dcconcept.cz
support@dcconcept.cz

Datum aktualizace: **1.11.2002**

Obsah:

1. Úvod

Manuál je určen vývojářům a konzultantům provádějícím modifikace, implementaci a podporu IS QI.

Předpokládané znalosti:
V rozsahu látky obsažené v prezentacích **Technologie** (015), minimálně však: architektura IS, terminologie, základy QI DNT, základní znalost funkčního objektu „Datový řez“, ovládání uživatelského rozhraní.
Použité zkratky a základní pojmy jsou definovány ve **Slovníku QI**.

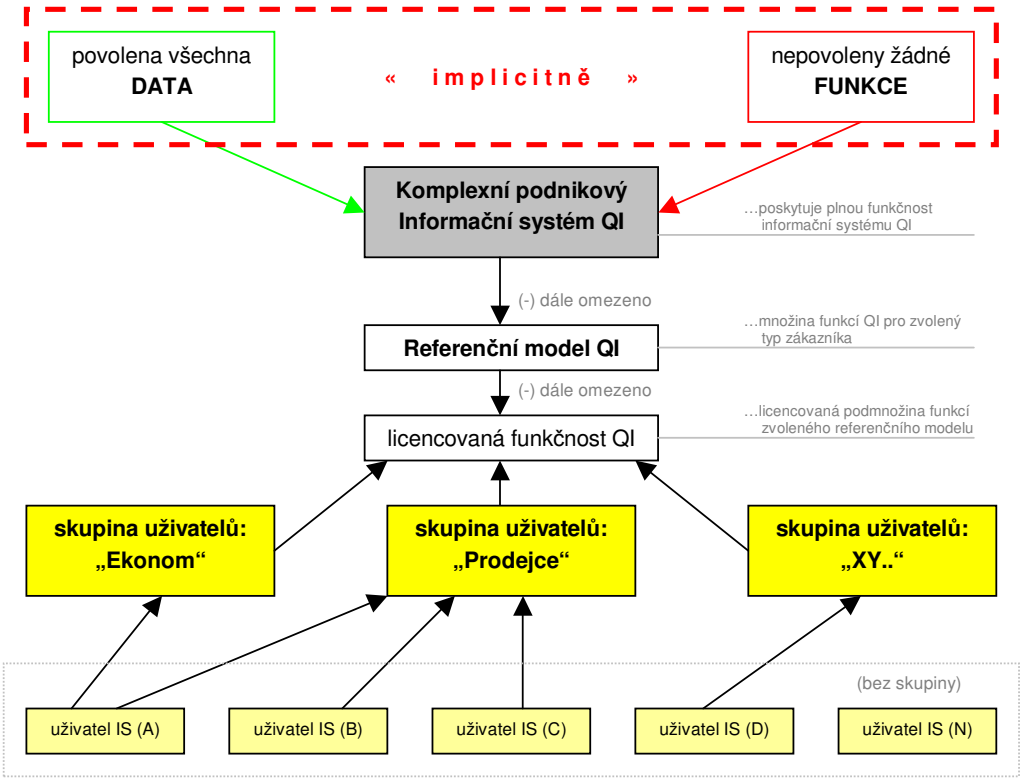
2. Přístupová práva

2.1. Přístupová práva v QI

Přístupová práva (dále jen PP) představují nástroj sloužící k definici pravidel pro práci s určitým objektem v informačním systému. Přidělují se uživateli nebo skupině uživatelů.
Přístupová práva se vztahují :

- **k programové funkci** (formulář, tiskový výstup, makro,..)**,**
- **k množině dat.**

Princip omezování / povolování přístupu:



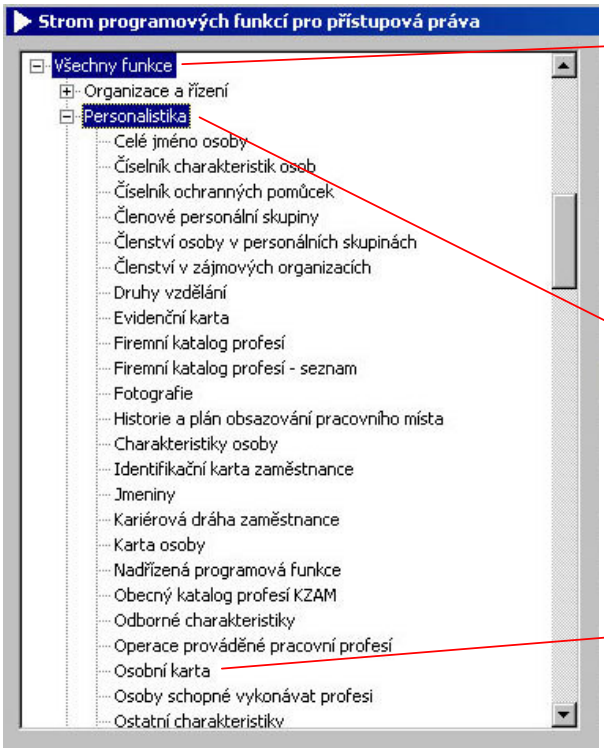
2.1.1. Strom PF

Pro práci s přístupovými právy je směrodatná **struktura Stromu PF**. Slouží k zobrazení všech programových funkcí formou hierarchického stromu, kde jednotlivé PF jsou rozčleněny do množin (v tomto případě **kořenů**). Dle této hierarchie se také řídí vyhodnocování přístupových práv.

Ve vztahu k definici PP platí pravidla:

- povolením / zákazem kořene PF jsou povoleny / zakázány všechny PF v něm zahrnuté, tzn. jemu podřízené (příkl. 1, 2),
- povolení / zákaz PF v rámci kořene PF se vztahuje pouze k této PF (příkl. 3).

Příklad stromového zobrazení PF:



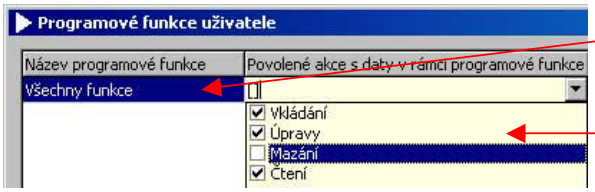
Příklad 1: povolení / zákaz kořene „*Všechny funkce*“ povolí / zakáže všechny podřízené úrovně, tj. celý strom PF.

Příklad 2: povolení / zákaz konkrétního kořene (např. „Personalistika“) povolí / zakáže všechny jemu podřízené úrovně.

Příklad 3: povolení / zákaz konkrétní PF povolí / zakáže pouze tuto PF. Ostatní PF v rámci kořene toto PP neovlivní.

- pro každý kořen PF / každou PF lze nadefinovat povolené operace,

Příklad definice povolených operací:



Zde vybrat PF (resp. kořen PF), pro kterou budou povolovány / omezovány operace.

Zde určit, které operace budou povoleny (zaškrtnuto). Ostatní budou zakázány.

2.1.2. Obecná pravidla pro práci s přístupovými právy

V systému QI obecně platí následující pravidla při využívání přístupových práv:

- **nenaplněná PP k programovým funkcím** implicitně zakazují přístup na všechny programové funkce,
- **nenaplněná PP na data (datové třídy)** implicitně povolují přístup na všechna data.

To znamená, že uživatel bez přidělených přístupových práv je sice oprávněn pracovat s veškerými daty systému, ale nemá k dispozici žádné funkce, kterými by tento přístup mohl realizovat.

Hlavní nabídka informačního systému QI pak pro takového uživatele nemá žádné položky.

2.1.3. Základní logika přístupových práv

Definice přístupových práv umožňuje využití dvou základních přístupů, jsou to následující pohledy:

- **zakazovací logika** (povolit větší množinu funkcí a v rámci ní zakazovat menší množiny či konkrétní funkce),
- **povolovací logika** (přímo povolovat množiny funkcí / konkrétní funkce).

Volba konkrétní logiky pak vychází z analýzy struktury organizace a analýzy procesů a jednotlivých činností členů organizace – uživatelů IS.

2.1.4. Povolené operace s objektem

Přístupová práva je možno definovat v **několika stupních**, opravňujících uživatele k vykonávání operací s daným objektem v rámci zvolené funkce.
Jsou to operace:

- **čtení**,
- **vkládání**,
- **úpravy**,
- **mazání**.

Poznámka: v případě atributů datové třídy jsou dostupné pouze operace: čtení, úpravy.

2.2. Správce přístupových práv

Přístupová práva pro jednotlivé uživatele IS (resp. skupiny) je v informačním systému QI oprávněn definovat pouze uživatel **Admin**. Tento uživatel je do QI vložen výrobcem, implicitně bez přístupového hesla (nutno zadat dodatečně).

2.3. Uživatel IS

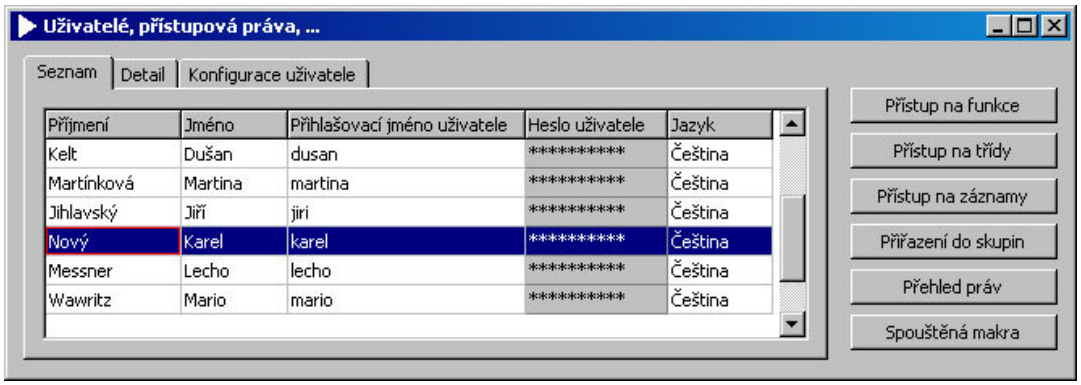
Za **Uživatele informačního systému** je považovaná **osoba evidovaná v databázi informačního systému, která má do něj povolen přístup**. Přístup je definován a chráněn uživatelským jménem a heslem.
Každý uživatel může se systémem QI pracovat v **jiném jazyce** uživatelského rozhraní a **používat odlišnou konfiguraci**.

2.3.1. Formulář „*Uživatelé, přístupová práva..*“

Založení nového uživatele IS se provádí na formuláři „*Uživatelé, přístupová práva..*“ výběrem ze seznamu osob. Tento formulář rovněž umožňuje definici PP uživatele (prostřednictvím příslušných tlačítek). Pro každého uživatele IS lze takto nastavit PP na programové funkce, na datové třídy a jejich atributy, a na záznamy.

2.3.2. Založení nového uživatele IS

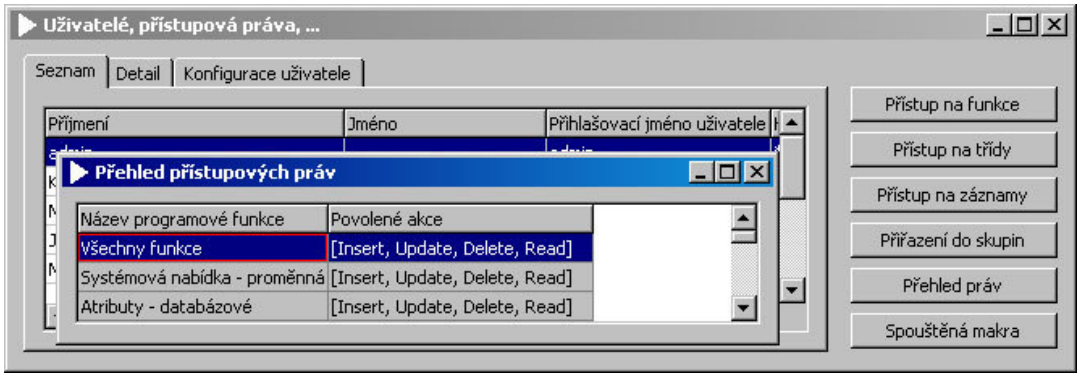
Založení nového uživatele IS se provádí na formuláři „*Uživatel, přístupová práva..*“:



Formulář je vyvolán z **Hlavní nabídky** (Konfigurace a správa systému) a jsou na něm umístěná tlačítka, která umožňují:

- přiřadit uživateli PP na funkce, datové třídy a atributy, na záznamy,
- přiřadit uživatele do jedné nebo více skupin,
- přiřadit uživateli spouštění maker.

Přehled **všech přístupových práv uživatele** lze vyvolat tlačítkem **Přehled práv** na tomto formuláři:



2.4. Skupina uživatelů IS

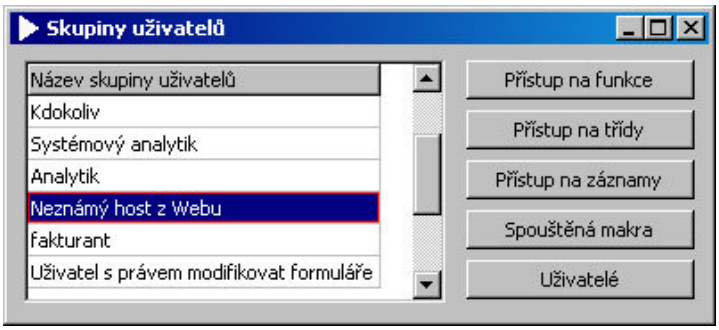
Hovoříme-li o **Skupinách uživatelů** v QI, máme na mysli **skupiny uživatelů informačního systému sloužící k usnadnění přidělování přístupových práv**.
Přiřazením skupiny k uživateli je zajištěna dědičnost PP (tzn. uživatel má povolena PP příslušící jemu přiřazené skupině uživatelů). Každý uživatel může být zařazen do více skupin, jejich PP se vzájemně prolínají – u PP na funkce má vyšší prioritu má právo povolovací, u PP na data právo zakazovací..

2.4.1. Formulář „*Skupiny uživatelů*“

Podobně jako v případě uživatele IS, také pro každou skupinu lze nastavit PP na programové funkce, třídy a záznamy. Tato PP se nastavují prostřednictvím příslušných tlačítek na formuláři „*Skupiny uživatelů*“ (viz dále).

2.4.2. Založení nové skupiny uživatelů

Založení nové skupiny uživatelů IS se provádí vložením nového záznamu na formuláři „*Skupiny uživatelů*“:



Formulář je vyvolán z **Hlavní nabídky** (Konfigurace a správa systému). Jsou na něm umístěna tlačítka, která umožňují:

- přiřadit skupině PP na funkce, datové třídy a atributy, na záznamy,
- přiřadit skupině spouštění maker,
- volbou tlačítka **Uživatelé** vyvolat přehled přiřazených uživatelů, včetně možnosti hromadného zařazení uživatelů do skupiny.

2.4.3. Zařazení uživatele do skupiny

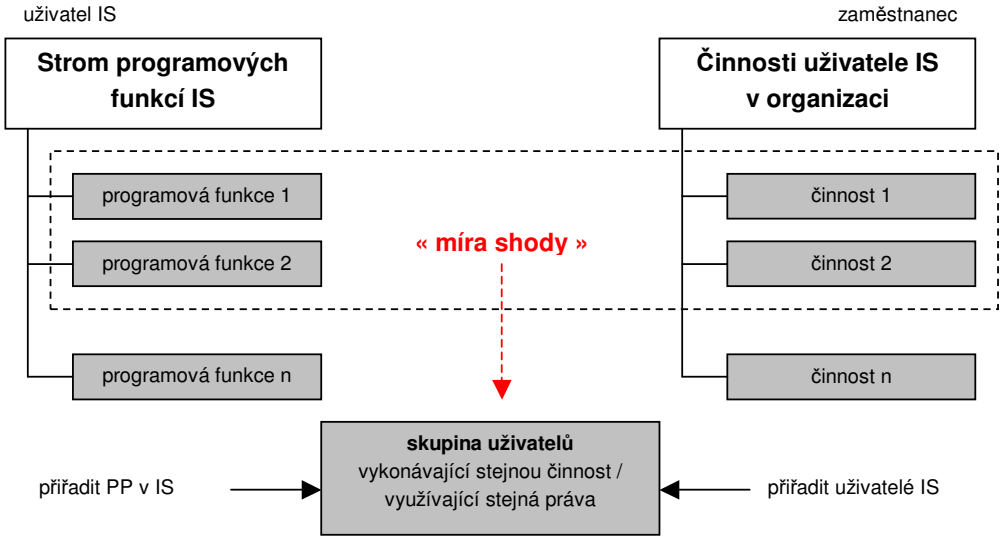
Volbou tlačítka **Uživatelé** na formuláři „*Skupiny uživatelů*“ je vyvolán seznam všech přiřazených uživatelů. Přidáním nového záznamu na tomto seznamu (výběrem ze seznamu osob) je zajištěno přiřazení tohoto uživatele do aktuální skupiny (včetně její PP). Přičemž platí pravidlo, že každý uživatel může být zařazen do více skupin a naopak do každé skupiny může být zařazen libovolný počet uživatelů.

3. Princip práce s přístupovými právy

Efektivní definice přístupových práv pro jednotlivé uživatele (a skupiny uživatelů) konkrétního informačního systému v organizaci **vyžaduje podrobnou analýzu procesů a jednotlivých činností v organizaci a v ní platných pravidel práce s daty**.
Vlastní princip přiřazování přístupových práv vychází z předpokladu, že **uživatel IS** je také **člen organizace** (zaměstnanec) zmocněn k určitým činnostem, k jejichž naplňování potřebuje zpřístupnit určité specifické skupiny dat, resp. programových funkcí zpřístupňující tyto skupiny dat. Dále je potřeba rozlišovat, jaká **úroveň přístupu** (operace: *čtení, vkládání, úpravy, mazání*) na tato data je pro daného uživatele nezbytná. Z toho vyplývá, že v případě definice přístupových práv pro organizaci dochází ke konfrontaci mezi dvěma strukturami:

- **struktura organizace** (činnosti jednotlivých členů organizace = uživatelů IS)
- **struktura programových funkcí IS** (konfigurace stromu programových funkcí v IS)

Poznámka: Je možné nastavit PP i osobě, která není členem organizace, která IS provozuje.



Výsledkem je stav, kdy dochází k určité shodě mezi požadavky zajištění přístupu na data (spojené s vykonáváním určitých činností) a programovými funkcemi IS zpřístupňujícím tato data uživateli IS.

Měl by být dodržen následující postup:

1. **analýza organizace** ve vztahu přístupu členů organizace k datům,
2. **definice optimální struktury přístupových práv** pro danou organizaci a její členy,
3. **definice skupin uživatelů** využívajících stejná přístupová práva (např. ekonom, prodejce..),
4. **přiřazení konkrétních uživatelů** do skupin (tzn. konkrétní osoby v organizaci),
5. přiřazení (resp. omezení) **individuálních přístupových práv** konkrétnímu uživateli ve skupině.

Čím je shoda mezi požadavky skupiny (uživatele) a konfigurací programových funkcí v rámci stromu PF vyšší, o to je vhodnější volba tzv. **zakazovací logiky** (tj. povolit skupině celý strom či kořen PF a zakazovat dílčí programové funkce v něm).
Naopak vysoká míra neshody je předpokladem pro volbu **logiky povolovací** (povolovat pouze určité PF či kořeny PF).

Přičemž je potřeba brát ohled na skutečnost, že:

- každý uživatel IS může **mít přiřazeno více skupin** uživatelů,
- přístupová práva takto přiřazených skupin uživateli se **prolínají**,
- a **povolovací právo je silnější než zakazovací u PP na PF**, naopak **povolené PP na data je silnější právo zakazovací**.

4. Přístupová práva na funkce

Přiřazení přístupových práv uživateli (resp. skupině uživatelů) na programové funkce se provádí pomocí příslušných tlačítek **Přístup na funkce** na formuláři „*Uživatelé, přístupová práva..*“ (resp. „*Skupiny uživatelů*“). Postup přiřazení PP pro jednotlivé uživatele i skupiny probíhá podle stejného modelu, s tím rozdílem, že přiřazením uživatele ke skupině tento uživatel ke svým PP přebírá také práva přiřazené skupiny (resp. skupin).

Postup definice přístupu na PF (funkce zpřístupňující data IS):

1. z **Hlavní nabídky / Konfigurace a správa systému** vyvolat příslušný formulář „*Uživatelé, přístupová práva..*“ (resp. „*Skupiny uživatelů*“),
2. volbou tlačítka **Přístup na funkce** vyvolat formulář určený k výčtu programových funkcí nebo kořenů stromu přístupových práv k povolení či zakázání přístupu k programovým funkcím,
3. přidáním nového záznamu do tohoto seznamu vybrat požadovanou PF,
4. v příslušném údaji tlačítkem vyvolat z výčtu povolených operací k vybrané PF (vkládání, úpravy, mazání, čtení) – platí pravidlo:
   nezaškrtnutí žádné operace k PF = zákaz PF
5. takto sestavenou definici PP uložit tlačítkem systémové nabídky.

5. Přístupová práva na třídy a atributy (data IS)

Vlastní přiřazení přístupových práv uživateli (resp. skupině uživatelů) na datové třídy a v nich obsažené atributy se provádí v podstatě podle stejného schématu jako v případě PF – v tomto případě tlačítky **Přístup na třídy**:

1. z **Hlavní nabídky / Konfigurace a správa systému** vyvolat příslušný formulář „*Uživatelé, přístupová práva..*“ (resp. „*Skupiny uživatelů*“),
2. volbou tlačítka **Přístup na třídy** formulář určený k výčtu datových tříd pro povolení či zakázání přístupu k datům,
3. přidáním nového záznamu do tohoto seznamu vybrat požadovanou datovou třídu,
4. v příslušném údaji tlačítkem vyvolat z výčtu povolených operací k vybrané datové třídě (vkládání, úpravy, mazání, čtení) – platí pravidlo:
   nezaškrtnutí žádné operace k datové třídě = zákaz práce s touto datovou třídou
5. případně volbou tlačítka **Přístup na atributy** určit specifická omezení (povolení) přístupu na jednotlivé atributy v seznamu označené datové třídy, včetně určení stupně přístupu na tyto atributy (k dispozici pouze operace: úpravy, čtení),
6. takto sestavenou definici PP uložit tlačítkem systémové nabídky.

Příklad 1: **Zakázat danému uživateli zobrazování rodných čísel - u Osob.**

Řešení:

1) na formuláři „*Uživatelé, přístupová práva..*“ najít uvedeného uživatele a vybrat,
2) tlačítkem Přístup na třídy zobrazit dialog pro definici PP,
3) do seznamu tříd vybrat třídu *Osoby* a na ní povolit všechny dostupné operace,

4) volbou tlačítka **Přístup na atributy** vybrat atribut *Rodné číslo* a pro něj nepovolit žádnou operaci (= zakázat atribut).

Popisovaná definice způsobí, že uvedený uživatel po přihlášení do systému nebude mít k dispozici náhled na rodná čísla osob – tento údaj se nebude na příslušných formulářích vůbec zobrazovat.

Příklad 2: **Zakázat danému uživateli editaci rodných čísel - u Osob.**

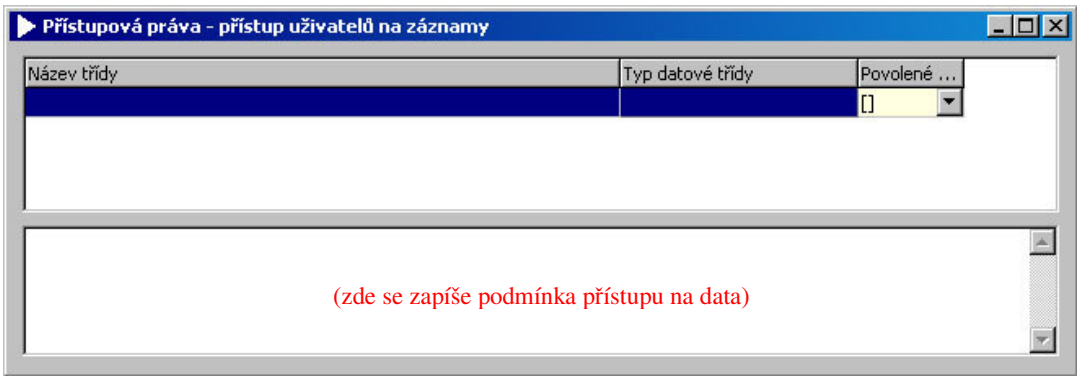
Řešení:

1) na formuláři „*Uživatelé, přístupová práva..*“ najít uvedeného uživatele a vybrat,
2) tlačítkem Přístup na třídy zobrazit dialog pro definici PP,
3) do seznamu tříd vybrat třídu *Osoby* a na ní povolit všechny dostupné operace,
4) volbou tlačítka **Přístup na atributy** vybrat atribut *Rodné číslo* a pro něj povolit pouze operaci čtení.

Popisovaná definice způsobí, že uvedený uživatel po přihlášení do systému sice bude mít k dispozici náhled na rodná čísla osob – nikoliv však k modifikaci (údaj v šedém „needitovatelném“ poli).

6. Přístupová práva na záznamy

Definice PP na záznamy umožňuje určit, ke kterým údajům IS bude mít uživatel (resp. skupina) přístup. K určení definice PP na záznamy slouží příslušné tlačítko Přístup na záznamy:



Horní polovina takto vyvolaného dialogu „*Přístupová práva – přístup uživatelů na záznamy*“ (v případě skupin analogicky“ *přístup sk. uživatelů na* záznamy) slouží k zadání **datové třídy** a přiřazení k ní povolených operací. Dolní část obsahuje **Podmínku v přístupech na data**.

Poznámka: Syntaxe Filtru je jako u datového řezu jen údaj ve dvojitých uvozovkách je potřeba definovat jinak, a to :

- systémová pole : ic,u,ic_a,u_a,ic_b,u_b
- nesystémová pole : ID (IC,U) atributu z tabulky atributů

Multijazyčné atributy v těchto filtrech nejsou povoleny. Žádná použitá identifikace objektu nesouvisí s datovým řezem.

6.1. Postup nastavení PP na záznamy

Schématický metodický postup nastavení přístupových práv na záznamy:

1) **zjištění datových řezů** z formulářů, které mají PP na záznamy aplikovat,
2) z datových řezů **najít objektovou třídu**, jejíž atribut má být předmětem PP,
3) v seznamu atributů si **zjistit ic,u požadovaného atributu** (uložen v ic_b, u_b v seznamu všech atributů),
4) **nastavení PP** na atribut třídy do PP na záznamy uživateli či skupině uživatelů.

Pro zadávání výběrové podmínky přístupových práv na záznamy se zadávají vybrané příkazy MS SQL Serveru, uvedeny v nápovědě. Podrobný popis těchto funkcí je součástí dokumentace SQL Serveru.

Další podmínky:

- atributy se zadávají ve tvaru: "ic,u",
- řetězce v apostrofech,
- lze použít ic,u atributů z nadřízených objektových tříd.

Důležité: Ideální je volit filtraci na povinné atributy povinné objektové třídy nebo metodicky zajistit plnění těchto atributů uživatelem (jedná se hlavně o atributy relačně vázaných tříd).
Příklad: středisko je na dokladech nepovinné a pokud není zadáváno, nelze přístupovými právy zamezit přístupu k dokladům s nezadaným střediskem.

6.2. Příklad nastavení PP na záznamy

Nastavit PP na vydané dodací listy střediska 000:

- formulář: „*Seznam dodacích listů vydaných*“
- datový řez: "Dodací listy vydané"
- objektová třída: Hospodářská střediska
- atribut: **Identifikace hosp. střediska** (34817,10)

Řešení:
Do PP na záznamy zvolit třídu "Hospodářská střediska" a povolené akce DS nechat prázdné.
Příkaz:

```
Case when "34817,10" = '000' Then 1 Else 0 End = 0
```

místo příkazu Case ... lze použít i příkaz:

```
"34817,10" <> '000'
```

ten ale nezohledňuje hodnotu „null“ v existující identifikaci hospodářského střediska (pokud by byla povolena při vstupování středisek), je důležité si uvědomit, pokud by na dokladu nebyla vůbec vazba na středisko (uživatel jej prostě nezadal protože není povinné), doklady bez střediska budou zpřístupněny vždy.

Analogicky lze řešit řízení přístupu k dokladům přes řady, typy a podtypy (objektová třída "Typy a podtypy dokladů" a její atributy).

7. Spouštění maker

IS QI umožňuje nadefinovat, která makra se budou pro daného uživatele IS (resp. skupinu) spouštět po přihlášení do systému (např. dnešní výročí nebo úkoly uživatele atd.; pro správce systému např. protokoly o spouštění apod.). Tato definice se realizuje prostřednictvím tlačítka **Spouštěná makra** na formuláři „*Uživatele, přístupová práva..*“ (resp. „*Skupiny uživatelů*“).

8. Příklad konstrukce uživatelského přístupu na PF

8.1. Časté chyby

Dále uvedený postup tvorby a přiřazování přístupových práv v informačním systému QI vychází z praktických zkušeností a umožňuje eliminaci častých chyb:

- uživateli nebylo přiřazeno určité PP potřebné k využití určité PF (např. výběr z číselníku),
- uživateli byly nedopatřením povoleny PP, které nemůže mít k dispozici (např. přiřazením více skupin),
- uživatel sice má přiřazeno určité PP, ale s nedostatečným výčtem povolených operací (např. umožňuje pouze na čtení),
- nebo naopak uživatel má povoleno PP na vyšší úrovni, než je pro něj přípustné (např. může mazat existující záznamy).

8.2. Postup konstrukce uživatelského přístupu

8.2.1. Výchozí předpoklad

Popisovaná metoda vychází z předpokladu, že správce přístupových práv bude do IS přihlášen současně pod svým, **administratorským účtem (dále QI-1)** a pod **účtem uživatele (dále jen QI-2)**, pro kterého definuje PP. V případě skupiny uživatelů se přihlásí pod účtem fiktivního uživatele, jemuž byla skupina přiřazena.

8.2.2. Založení skupiny

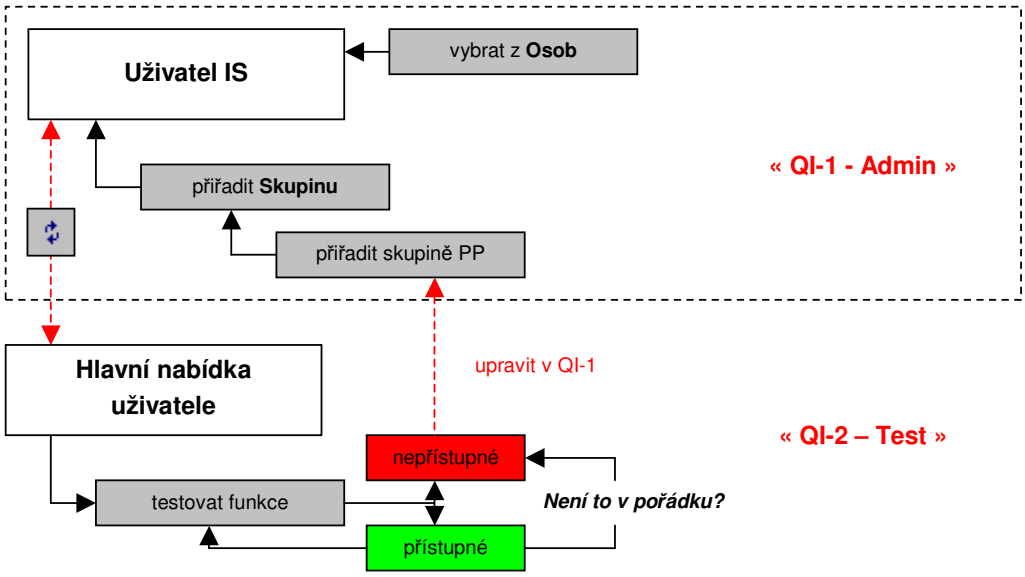
Za předpokladu současného přihlášení do systému QI-1 a QI-2 vlastní definice přístupových práv probíhá následovně:

1. **přihlásit se jako správce PP** (tj. QI-1),
2. v QI-1 **založit novou skupinu** uživatelů,
3. v QI-1 **založit nového uživatele**, pro kterého budou definovány PP (pokud již neexistuje), následně **přiřadit** tomuto uživateli dříve vytvořenou skupinu,
4. **přihlásit se do systému jako takto vytvořený uživatel** (tj. QI-2), aplikace QI-1 je spuštěna paralelně,
5. v QI-2 je hlavní nabídka prázdná – skupina nemá přiřazena žádná PP.

8.2.3. Definice PP pro skupinu

Vlastní přiřazování PP skupině (resp. uživateli) probíhá na základě následujícího algoritmu:

1. v QI-1 **přiřadit skupině požadované PP** a pro ně označit výčet povolených operací,
2. v QI-2 po obnovení obsahu nabídky se **změna projeví** zobrazením příslušného kořene PF, resp. konkrétních PF,
3. v QI-2 **testovat**, zda-li přiřazené PP uživateli poskytuje požadovanou funkčnost:
   - **pokud NE**, pak v QI-1 přiřadit vyžadované PP na příslušné úrovni (čtení,..),
   - **pokud ANO**, pak zvážit zda tento stav odpovídá požadované definici struktury PP:
     - **pokud NE**, pak v QI-1 upravit PP,
     - **pokud ANO**, pak pokračovat v testování funkčnosti,
4. pokud je v QI-2 fiktivnímu uživateli dostupná nabídka všech požadovaných PF na příslušné úrovni, lze definici PP pro skupinu (přiřazenou tomuto uživateli) považovat za dokončenou.



Poznámka: uvedený postup lze aplikovat i přímo na konkrétního uživatele IS, s vynecháním kroků spojených se vytvářením skupiny. Vzniká tak však riziko, že v budoucnu vznikne požadavek na zpřístupnění stejné (resp. velice podobné) definice PP dalšímu uživateli, což představuje pracné opakování celého cyklu.

Stav může nastat:

A) organizace přijme **dalšího člena**, jehož činnost vyžaduje v podstatě stejná PP,
B) dojde k **personální změně** na uvedené pracovní pozici, tzn. bude stávající uživatel nahrazen jiným.

Z tohoto pohledu **je vhodné vždy nadefinovat PP pro skupiny uživatelů** (podle struktury pracovních míst v organizaci) a jednotlivé koncové uživatele IS z řad členů organizace přiřazovat do těchto skupin (i když se jedná jen o jednu osobu).

8.2.4. Doladění PP pro jednotlivé uživatele

Detailní **přizpůsobení definice PP pro individuální potřeby konkrétního uživatele IS** probíhá na základě následujícího cyklu:

1. **přihlásit se jako správce PP** (tj. QI-1),
2. v Q1-1 **založit nového uživatele**, pro kterého budou definovány PP (pokud již neexistuje), následně **přiřadit** tomuto uživateli dříve vytvořeno skupinu obsahující vhodnou definici PP,
3. **přihlásit se do systému jako takto vytvořený uživatel** (tj. QI-2), aplikace QI-1 je spuštěna paralelně (pro zjednodušení práce doporučeno spustit opět na dvou stanicích),
4. v QI-2 je **hlavní nabídka odpovídá PP přiděleným přiřazené skupině** – uživatel doposud nemá přiřazena žádná PP,
5. v QI-1 **přiřadit / omezit uživateli požadované PP** (resp. s ním spojené operace),
6. v QI-2 po obnovení obsahu nabídky se **změna projeví** zobrazením příslušného kořene PF, nebo přímo konkrétních PF,
7. v QI-2 **testovat**, zda-li přiřazené PP uživateli poskytuje požadovanou funkčnost:
   - **pokud NE**, pak v QI-1 přiřadit vyžadované PP na požadované úrovni (čtení,..),
   - **pokud ANO**, pak zvážit zda tento stav odpovídá definici struktury PP:

- **pokud NE**, pak v QI-1 upravit PP,
- **pokud ANO**, pak pokračovat v testování funkčnosti,

8. pokud v QI-2 je uživateli dostupná nabídka všech požadovaných PF na příslušné úrovni, lze definici PP pro tohoto uživatele považovat za dokončenou.

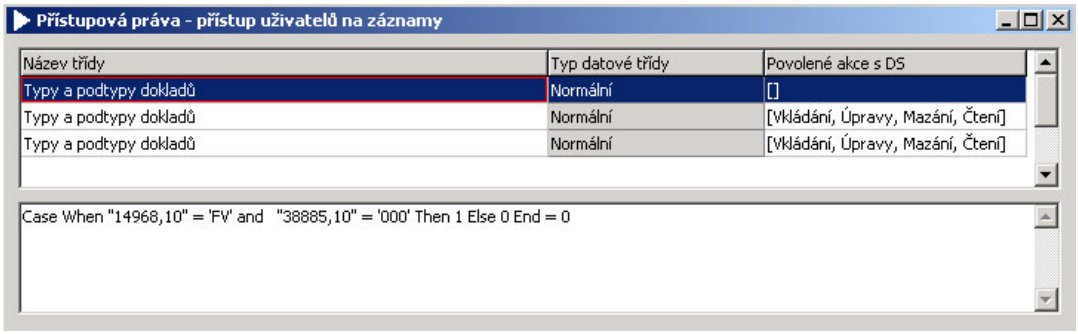
9. Příklady konstrukce přístupových práv na záznamy

Následující kapitoly popisují postup nastavení přístupových práv na záznamy.

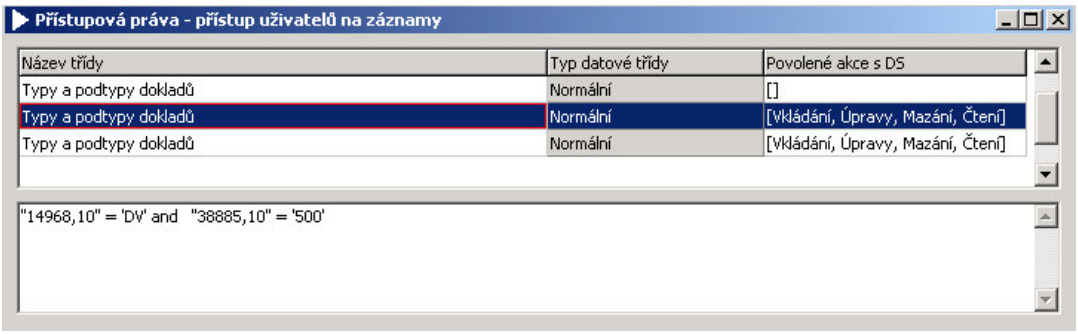
Poznámka: následující postupy jsou určeny pro vymezení vlastních dokladových podtypů, řad, skladů a pokladen uživatelům pracujícím na pobočkách v rámci distribuovaného zpracování dat.

9.1. Povolení přístupových práv na podtypy a řady

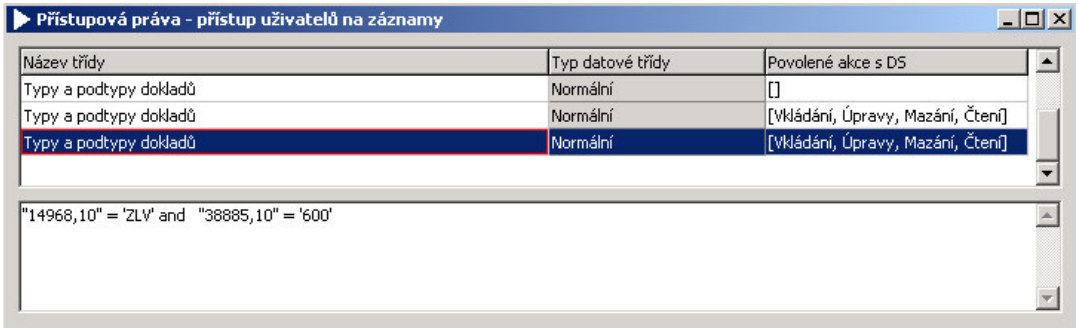
První záznam zakazuje zobrazení všech podtypů a řad kromě zadaného v podmínce. Postup nastavení PP na podtypy a řady dokladů odfiltrováním těch podtypů a řad, do kterých uživatel vůbec nesmí pořizovat data (tzn. faktura vydaná řady 000):



Další záznam povoluje přístup vydaným dobropisům řady 500:



Další záznam povoluje přístup vydaným zálohovým listům řady 600:

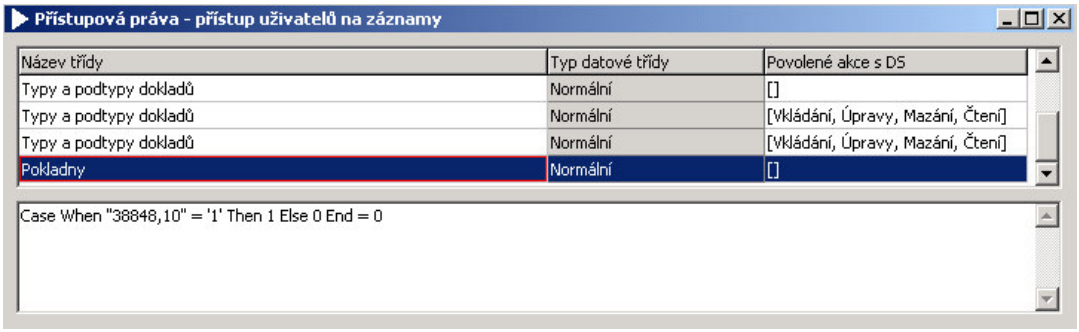


Další povolení vymezeného okruhu podtypů a řad se realizuje na základě stejného principu.

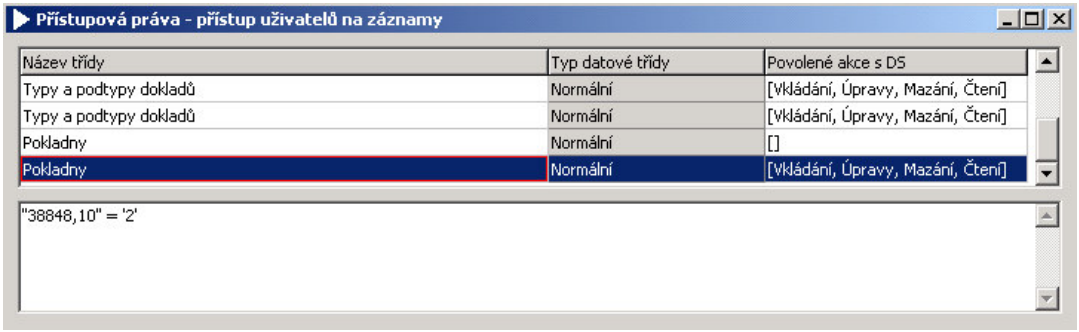
9.2. Přístupová práva na pokladny

9.2.1. Pokladny

Tento záznam zakazuje přístup do všech pokladen kromě pokladny 1, kde je plný přístup:



Tento záznam navíc povoluje plný přístup k pokladně 2:



Další povolení vymezeného okruhu pokladen se realizuje na základě stejného principu.

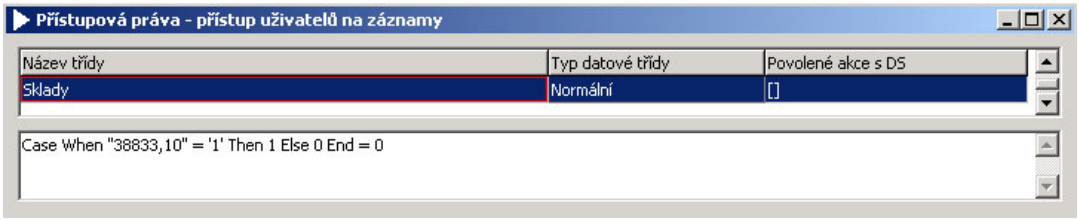
9.2.2. Podtypy a řady pokladních příjemek a výdejek

Nastavení přístupu na Podtypy a řady pokladních příjemek a výdejek je shodné s popisem první kapitoly této části manuálu.

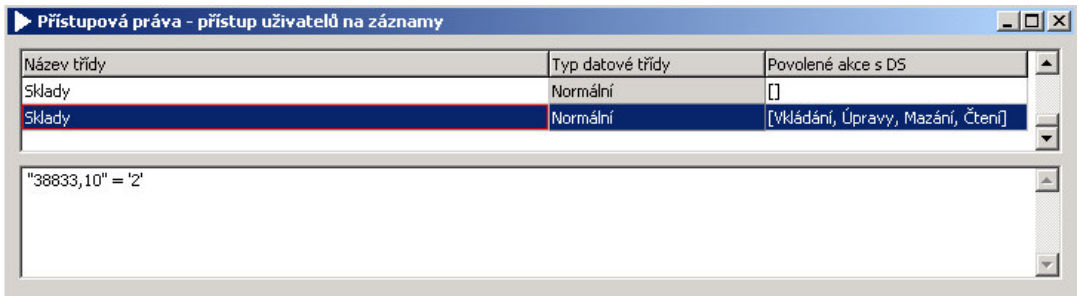
9.3. Přístupová práva na sklady

9.3.1. Sklady

Tento záznam zakazuje přístup do všech skladů kromě skladu 1, kde je plný přístup:



Tento záznam navíc povoluje plný přístup ke skladu 2:



Další povolení vymezeného okruhu skladů se realizuje na základě stejného principu.

9.3.2. Podtypy a řady skladových příjemek a výdejek (skladové pohyby)

Nastavení přístupu na Podtypy a řady skladových příjemek a výdejek je shodné s popisem první kapitoly této části manuálu.

9.4. Ilustrační případ

Zadání: Povolit všechny podtypy a řady všech typů, zakázat všechny podtypy a řady jednoho typu dokladu a povolit jeden z nich.

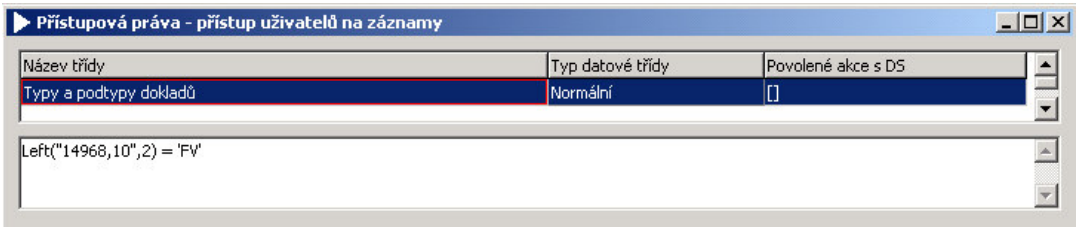
Předpoklad: Konstrukce zkratky dokladu všech podtypů jednoto typu dokladu má společný základ, který je v rámci všech existujících typů dokladů jedinečný, na příkladě se uvažuje se společným základem 2 znaků zleva.

9.4.1. Povolit všechny podtypy a řady všech typů

Je standardně splněno, pokud nejsou zadána přístupová práva na záznamy dané třídy.

9.4.2. Zakázat všechny podtypy a řady jednoho typu dokladu

Příklad: Zákaz přístupu ke všem podtypům začínajících zkratkou dokladu „FV“, ostatní podtypy jsou plně přístupné:



9.4.3. Povolit používání jednoho podtypu z množiny zakázaných

Příklad: Ze zakázaného přístupu ke všem podtypům začínajících zkratkou dokladu „FV“ je potřeba zpřístupnit jeden se zkratkou „FVS“: