OpenID služba CZ.NIC

Specifikace zavedení OpenID do registru domén

Verze 1.0

23.10.2009

Obsah

O OpenID

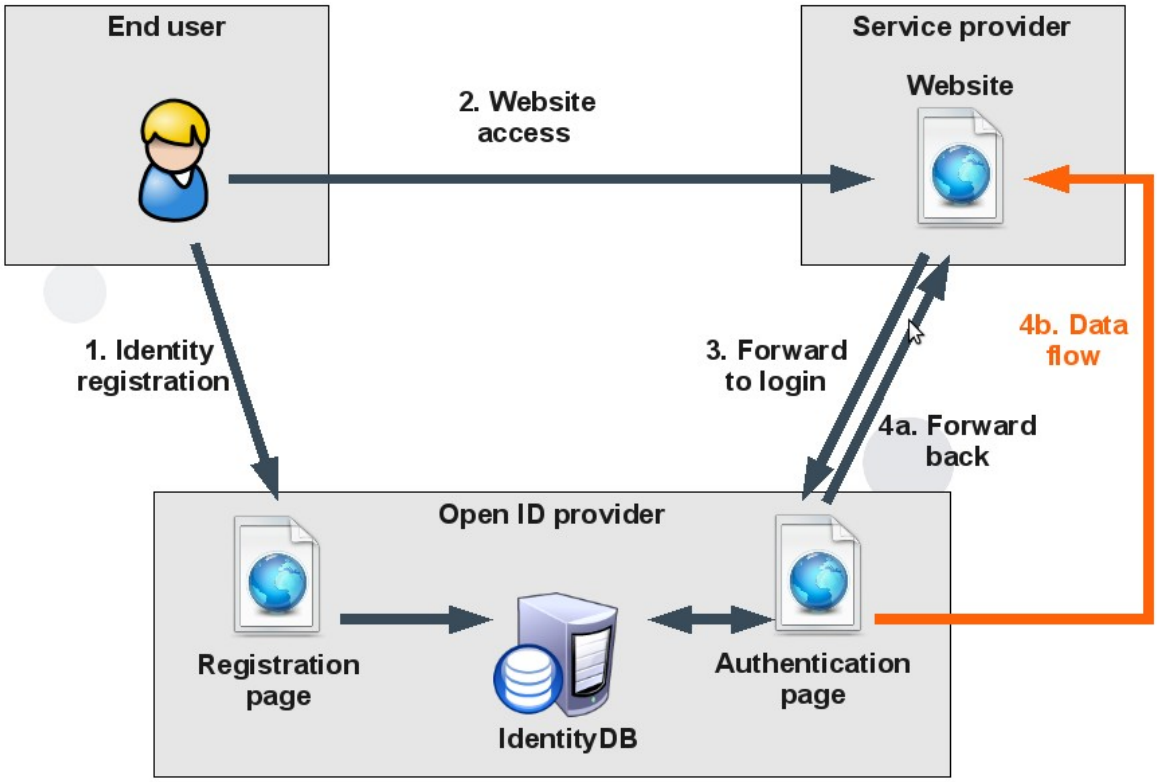
Co je OpenID

OpenID je otevřený decentralizovaný a svobodný systém pro správu elektronické identity. OpenID je technologie, která nabízí uživatelům internetu možnost používat jednotné identifikační údaje (uživatelské jméno a heslo) pro více různých webových stránek. Odstraňuje tak potřebu se na každých konkrétních webových stránkách registrovat a zakládat si účet. Vývoj OpenID protokolu zajišťuje nadace OpenID Foundation. Současná verze protokolu má číslo 2.0.

Jak OpenID funguje

OpenID funguje tak, že uživatel si u poskytovatele OpenID identity (tzv. OpenID provider) založí svoji identitu a získá tak svůj OpenID identifikátor. Tento identifikátor použije pro přihlášení na všech webových stránkách poskytovatelů služeb, které OpenID podporují. Autentizaci uživatele pak provádí příslušný poskytovatel OpenID identity. Celý proces přihlašování probíhá takto (viz následující obrázek):

1. Uživatel si založí svoji identitu u poskytovatele služby, tím získá tzv. OpenID identifikátor, který jednoznačně identifikuje jeho OpenID identitu. Údaje, které ke své identitě uvede, se uloží do databáze identit.
2. Uživatel otevře příslušnou webovou stránku, která podporuje přihlášení pomocí OpenID a do přihlašovacího okna vyplní svůj OpenID identifikátor místo běžné kombinace uživatelského jména a hesla a stiskne tlačítko pro přihlášení.
3. Aplikace podle vloženého identifikátoru vyhledá poskytovatele identity (tzv. proces „discovery“), který identifikátor poskytl. Od příslušného OpenID poskytovatele získá URL pro autentizaci, kam přihlašujícího se uživatele přesměruje. Na autentizační stránce OpenID poskytovatele uživatel provede přihlášení pomocí příslušné přihlašovací metody (nemusí být pouze běžné přihlášení pomocí hesla). K ověření uživatele dojde pomocí údajů z databáze identit.
4. Po provedení autentizace je uživatel přesměrován na původní stránku služby, kam se přihlašoval. Mezi tím je aplikace, která tuto službu poskytuje bočním kanálem informována o výsledku autentizace a může také obdržet další data o uživateli poskytnutá z databáze identit. V momentu, kdy se dokončí přesměrování uživatele zpět, provede se mu na stránkách příslušné služby přihlášení (v případě pozitivního výsledku) nebo mu je zobrazena chybová hláška, že přihlášení se nezdařilo (v případě negativního výsledku).



Obr.: Princip fungování OpenID

Technologie je podobná systémům Single Sign-On, ale je jednodušší na použití, protože používá otevřené technologie. Zároveň zde není potřeba instalace dodatečných programů ani žádných proprietárních protokolů. Decentralizace protokolu umožňuje svobodný výběr poskytovatele identity. Další informace o systému je možné nalézt na http://openid.net

Systém OpenID stanovuje pouze základní postup a pravidla pro provedení ověření identity uživatele mezi OpenID providerem a poskytovatelem služby. Vše ostatní, jako konkrétní metoda autentizace uživatele v systému OpenID providera či typ a obsah dat, která si mezi sebou v případě úspěšné autentizace uživatele předají, závisí na konkrétní implementaci u OpenID providera.

Proč OpenID v registru domén

Sdružení CZ.NIC bude implementovat OpenID do registru domén a zavádět službu OpenID, protože má na rozdíl od jiných potenciálních poskytovatelů OpenID identit a jiných služeb pro jednotnou autentizaci unikátní výhody.

Přirozené rozšíření služeb registru domén

Již dnes jsou v registru domén vedeny osoby jako tzv. kontakty, které reprezentují reálné uživatele. Kontakt obsahuje běžné údaje, které identifikují příslušnou osobu, jako jsou jméno (osoby samotné a nebo organizace, se kterou je osoba spojena), adresu, datum narození, číslo OP/pasu, e-mail, telefonní číslo apod. Některé z těchto údajů jsou veřejné, jiné nejsou, u některých záleží také na uživateli, zda je chce či nechce zveřejnit. Tyto kontakty jsou přiřazovány k doménám v různých rolích:

- Držitelé domén
- Administrativní kontakty
- Technické kontakty (a to ve smyslu spravující DNS či spravující DNSSEC)

Tyto kontakty mají již dnes v registru své vlastní heslo. Toto heslo slouží k tzv. transferu kontaktu, tedy ke změně určeného registrátora kontaktu. Tím je registrátor, který jako jediný může měnit údaje v registru u tohoto kontaktu. V praxi to je registrátor, kterého si uživatel vybral jako „správce“ svých údajů v registru a jemuž důvěřuje.

Z výše uvedeného je evidentní, že registr domén již dnes obsahuje identity osob (=kontakty) a autentifikační metody (=heslo pro transfer). Tyto identity mají zatím význam a funkci pouze pro popis vztahů osob k doménám, autentifikační metoda slouží pouze k ověření změny určeného registrátory. Je tedy nasnadě umožnit uživateli – osobě, která má svůj kontakt, využít záznamy v registru i pro další služby a umožnit další autentizační metody, jak pro tyto nové služby, tak samozřejmě i pro jedinou stávající službu.

OpenID je právě touto novou službou, která umožní využít obsah registru i pro obecnou identifikaci a přihlašování uživatelů pro jakékoliv webové služby.

Poptávka po neutrální službě se silným organizačním zázemím

OpenID služby, ve smyslu poskytování OpenID identit, už na trhu jsou či jsou takové služby a jejich podpora ohlášeny. A to nejen ze strany malých flexibilních organizací, ale i velkých poskytovatelů jako jsou např. Seznam či Google.

Problém malých poskytovatelů OpenID identit je v tom, že mají omezený dosah a omezenou důvěru uživatelů. Ti z pochopitelných důvodů nebudou chtít svěřit své osobní údaje jen tak nějaké „garážové“ firmě, protože nemohou mít jistotu, jak s jejich údaji bude naloženo či minimálně jestli tato firma dokáže zajistit co největší spolehlivost, dostupnost a bezpečnost takové OpenID služby. Stejné pochybnosti lze očekávat i u poskytovatelů webových služeb. Ti budou totiž opět z pochopitelných důvodů zvažovat, zda se jim vyplatí vkládat své zdroje do úprav své aplikace tak, aby nově podporovala OpenID identitu s relativně málo uživateli.

U velkých poskytovatelů je naopak značným problémem to, že záběr jejich činností je široký a je vysoce pravděpodobné, že se činnosti poskytovatele OpenID služby a poskytovatele webové služby, kde bude tato identita podporována, bude alespoň částečně shodovat. V takovém momentu nebudou chtít poskytovatelé internetových webových služeb chtít podporovat tuto OpenID identitu, protože při každém přihlášení uživatele získává správce OpenID identit digitální stopu uživatele. Tu může využít coby konkurenční prostředek; např. pokud poskytovatel identity získá v digitální stopě uživatele informaci, že se už po čtvrté za daný týden přihlašuje na stránku internetového obchodu s mobilními telefony, může toho marketingově využít a poslat mu speciální nabídku vlastních výrobků této kategorie.

CZ.NIC je organizace, která disponuje silným organizačním zázemím pro provoz služeb registru domén a má image stabilního a spolehlivého poskytovatele služeb. Navíc je z komerčního hlediska neutrální organizací, protože mimo provozu registrů domén neprovozuje žádné komerční činnosti. Proto je CZ.NIC jednou z mála možných organizací, které jako správci OpenID identity mají šanci všeobecně oslovit internetovou komunitu a trh a to jak ze stran koncových uživatelů identit, tak ze strany poskytovatelů internetových služeb, kteří budou tyto identity podporovat ve svých službách.

Služba pro širokou uživatelskou základnu

Problém s nutností vícenásobných registrací pro různé internetové služby a následné autentizace pomocí různých účtů, uživatelských jmen a hesel je obecným problémem internetu a neváže se pouze na nějakou vybranou skupinu uživatelů. To může být překážkou u komerčních poskytovatelů OpenID identit, kteří budou při poskytování OpenID identit motivováni komerčními důvody. To může přinášet různé specifické požadavky na uživatele či omezení, např. sociální (věk, schopnosti), nutností pořídit si nějaké další služby (nutnost mít email od poskytovatele identity), nutnost poskytovat údaje z identity dalším propojeným subjektům se správcem OpenID identity (např. pro marketingové účely) apod.

Jelikož motivací CZ.NIC je výhradně prospěch internetové komunitě, není tedy na místě obava, že by nějaký potenciální uživatel byl z jakéhokoliv důvodu diskriminován. Jedině služba provozována podobnou organizací jako je CZ.NIC může zajistit, že se k OpenID dostanou všichni uživatelé či skupiny uživatelů bez omezení.

Větší potenciál k masovému rozšíření

Služba OpenID ve svém základu zprostředkovává pouze autentizaci uživatelů. Tím, že OpenID umožňuje uživatelům používat stejné uživatelské jméno a heslo pro více různých služeb, přináší těmto uživatelům rozhodně nezanedbatelný přínos. Z hlediska poskytovatele nějaké internetové služby je ovšem tento přínos mnohem menší, protože pro něj znamená pouze to, že v momentu, kdy začne podporovat OpenID, se jeho potenciálními klienty stávají všichni uživatelé podporovaného správce OpenID identit. Tedy nejen ti uživatelé, kteří se zaregistrovali přímo ve službě samotné.

Poskytovatelé služeb ale řeší i další problémy s identitami uživatelů, které jim pomůže vyřešit jedna z unikátních vlastností OpenID služby CZ.NIC. Uživatelé se totiž mohou registrovat anonymně (se smyšlenými údaji) a to jak v systému poskytovatele, tak v systému běžného správce OpenID identit. To je např. problém pro poskytovatele služeb, kteří nabízejí elektronické obchody, kde by tito uživatelé mohli dělat falešné objednávky nebo např. pro internetové zpravodajské portály, na kterých uživatelé zneužívají své anonymity v tamních diskusích. Služba CZ.NIC bude mít unikátní vlastnost v tom, že bude motivovat uživatele k tomu, aby provedli ověření své identity. Uživatel OpenID identity bude mít možnost prokázat důvěryhodným způsobem svoji totožnost např. notářsky ověřeným podpisem nebo elektronickým podpisem a tudíž již nebude dále anonymní. Poskytovatel služby přijímající OpenID identity CZ.NIC bude pak mít k dispozici informaci, že dotyčná osoba opravdu existuje.

OpenID služba CZ.NIC proto bude daleko více atraktivnější pro poskytovatele webových služeb a má tak mnohem větší potenciál k masovému rozšíření, než když rozšíření bude „taženo“ pouze zájmem koncových uživatelů. Poskytovatelé služeb totiž mohou koncové uživatele také motivovat k používání OpenID.

Obecné charakteristiky OpenID služby

Poskytovatelé služeb

Poskytovatelé internetových služeb, kteří budou chtít využít OpenID systém CZ.NIC budou muset do svých aplikací integrovat ověřování a získávání údajů pomocí OpenID. Tato integrace znamená vývoj příslušné funkcionality v konkrétní aplikaci. Poskytovatelé služeb budou moci využít dva základní typy přístupu:

1. Základní přístup – Tento přístup bude moci využít kdokoliv z provozovatelů internetových služeb – nebude potřeba navázat žádný smluvní vztah ani se na tento typ přístupu nebudou vztahovat žádné speciální podmínky. Tento přístup bude zdarma. Při použití základního přístupu poskytne CZ.NIC poskytovateli služby pouze minimální sadu údajů o uživateli (pokud uživatel nestanoví sám jinak). Základní přístup se bude hodit pro obecné přihlašování stejnými údaji, kde není úplně nutné mít plně ověřenou identitu uživatele např. pro přihlašování do různých diskusních fór.
2. Rozšířený přístup – Pro získání tohoto přístupu bude potřeba uzavřít smlouvu mezi CZ.NIC a poskytovatelem připojení, která stanoví pravidla a podmínky získávání, používání a ochrany údajů v uživatelských identitách. Tento přístup do registru bude placený. Při použití tohoto přístupu bude mít poskytovatel služby možnost vyžadovat konkrétní metodu autentizace pro každý autentizační požadavek a získá po provedení autentizace uživatele k dispozici širší údajů o uživateli. Předpokládáme, že poskytovatelé služeb se budou rekrutovat zejména z následujících typů firem:
    - elektronické obchody
    - informační portály s diskusními fóry (média)
    - freemailové/webmailové služby
    - komunitní weby
    - interní systémy stávajících registrátorů

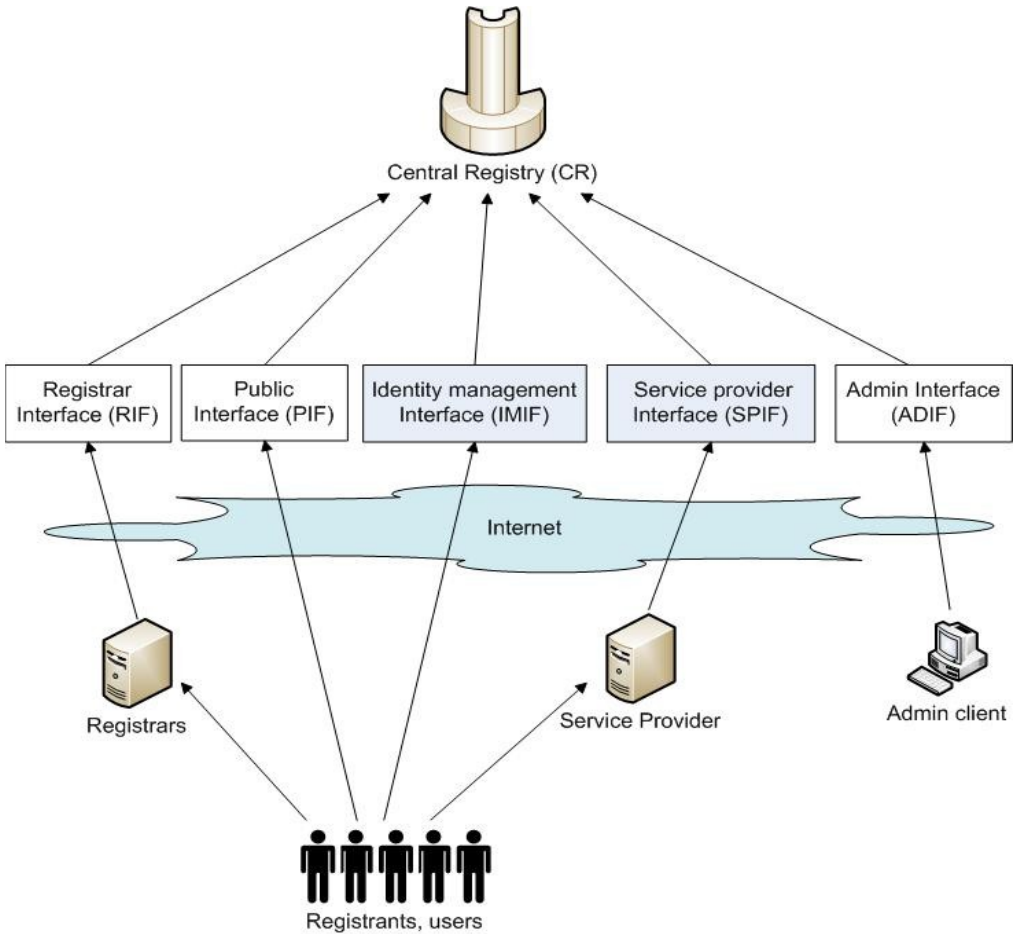
Bezpečnostní rizika

Z pohledu uživatele OpenID je bezpečnostním rizikem, že poskytovatelé OpenID identity mohou být častými cíly phishingu/pharmingu apod. a to, pokud dojde k masivnějšímu rozšíření OpenID. Získání identity OpenID bude „lákavější“, protože získání autentizačních údajů k OpenID identitě umožní potenciální přístup k více webovým aplikacím než získání uživatelského jména a hesla k jednomu konkrétnímu webovému systému. Z praktického hlediska k výraznému snížení bezpečnosti nedojde, protože je běžnou praxí, že uživatelé používají stejné uživatelské jméno a heslo na více webových stránkách. Decentralizace protokolu také klade větší zodpovědnost na uživatele při výběru poskytovatele identity. Nedůvěryhodný poskytovatel identity může být založen přímo za účelem získávání identit uživatelů. Z pohledu poskytovatele služby bezpečnostní rizika nehrozí, protože poskytovatel služby nemá autentizační údaje u sebe a ověření uživatele přenechává na poskytovateli OpenID identity.

Specifikace funkcionality OpenID služby CZ.NIC

Základní vlastnosti

Služba OpenID bude rozšířením stávajícího systému správy domén. OpenID identita bude rozšířením stávajícího objektu kontakt v centrálním registru. Takto rozšířený kontakt je dále nazýván identifikovaný kontakt. CZ.NIC bude zastávat roli registru OpenID. Vznikne nové rozhraní do centrálního registru implementující protokol OpenID, které budou využívat poskytovatelé služeb na internetu pro autentizaci svých uživatelů a nové rozhraní pro správu identifikovaných kontaktů. Systém správy domén pak bude odpovídat následujícímu schématu.



Obr.: Schéma systému správy domén

Následující seznam vypisuje jednotlivé komponenty rozšířeného registru správy domén, poskytujícího službu OpenID, které bude nutné vytvořit nebo upravit. Nejsou zde zahrnuty komponenty stávajícího systému, které se nemění, nebo které jsou součástí již uvedených komponent (generátor zóny, bankovní rozhraní apod.). Detail každé komponenty bude popsán v samostatné kapitole.

- **Centrální registr** V současném systému správy domén je centrální registr komponenta provádějící operace nad všemi objekty registru. Součástí centrálního registru bude databáze identit. V tuto chvíli jsou základními registrovatelnými objekty domény, kontakty, nssety a keysety. Centrální registr bude rozšířen o správu identifikovaných kontaktů a evidenci poskytovatelů služeb.
- **Rozhraní pro registrátory** Tímto rozhraním komunikují s centrálním registrem stávající registrátoři. Komunikace je obousměrná a registrátoři jsou tak informováni o změnách v jimi spravovaných objektech, pokud je sami nepožadovali. V rámci převodu běžného kontaktu na identifikovaný kontakt dojde k převodu kontaktu od registrátora a o této změně je registrátor informován tímto rozhraním.
- **Rozhraní pro veřejnost** Veřejnost má možnost přímo zjišťovat údaje z centrálního registru pomocí služeb whois. Dále má veřejnost možnost pomocí tohoto rozhraní vkládat do centrálního registru žádosti o provedení některých operací, které není možné provést přes registrátora. V souvislosti s OpenID bude upravena politika zveřejňování informací o kontaktech a přibudou některé nové statistiky.
- **Rozhraní pro administrátory** Rozhraní pro administrátory je aplikace, kterou používají správci systému (zaměstnanci CZ.NIC) k nastavení parametrů systému. V rozšíření pro OpenID bude tento systém nabízet administrativní úkony související se správou identifikovaných kontaktů a poskytovatelů služeb.
- **Rozhraní pro správu identifikovaných kontaktů** Přes toto webové rozhraní budou moci uživatelé registrovat a spravovat identifikované kontakty, převádět stávající kontakty na identifikované kontakty a žádat o validaci identifikovaných kontaktů. Rozhraní bude umožňovat automatizované předvyplnění údajů identifikovaného kontaktu.
- **Rozhraní pro poskytovatele služeb** Toto rozhraní slouží pro komunikaci s poskytovateli internetových služeb, kteří požadují autentizaci svých uživatelů. Komunikace na tomto rozhraní bude probíhat protokolem OpenID. V rámci této komunikace získají poskytovatelé služeb podrobnější informace o autentizovaných identifikovaných kontaktech. Součástí tohoto rozhraní bude webová aplikace pro zajištění vlastní autentizace.

Následující seznam popisuje externí uživatele systému.

- **Veřejnost** Veřejnost komunikuje s centrálním registrem buď prostřednictvím rozhraní pro veřejnost, nebo některého z registrátorů. V případě že využívá službu OpenID, komunikuje veřejnost s registrem prostřednictvím poskytovatele služeb nebo přes rozhraní pro správce OpenID.

- **Administrátoři** Administrátoři jsou zaměstnanci sdružení, kteří mají prostřednictvím rozhraní pro administrátory přístup k datům registru na základě jim přidělených oprávnění.
- **Poskytovatelé služeb** Poskytovateli služeb jsou myšleny systémy webových e-shopů, komunitních nebo zpravodajských serverů, kteří chtějí využívat tento OpenID systém pro jednotnou správu identit svých uživatelů. Tito poskytovatelé budou moci s využitím protokolu OpenID provádět prostřednictvím rozhraní pro poskytovatele služeb autentizaci svých uživatelů.
- **Registrátoři** Registrátor je právnická osoba, která má smluvní vztah s CZ. NIC a pouze jejímž prostřednictvím může veřejnost měnit údaje v centrálním registru.

Centrální registr

Centrální registr je klíčová komponenta systému. Jeho součástí je databáze spravující všechna data registru a nad ní aplikační vrstva, která zprostředkovává tato data do jednotlivých rozhraní. Vedle toho se zde nacházejí interní periodické procesy pro zajištění funkcionality systému.

Objekty centrálního registru

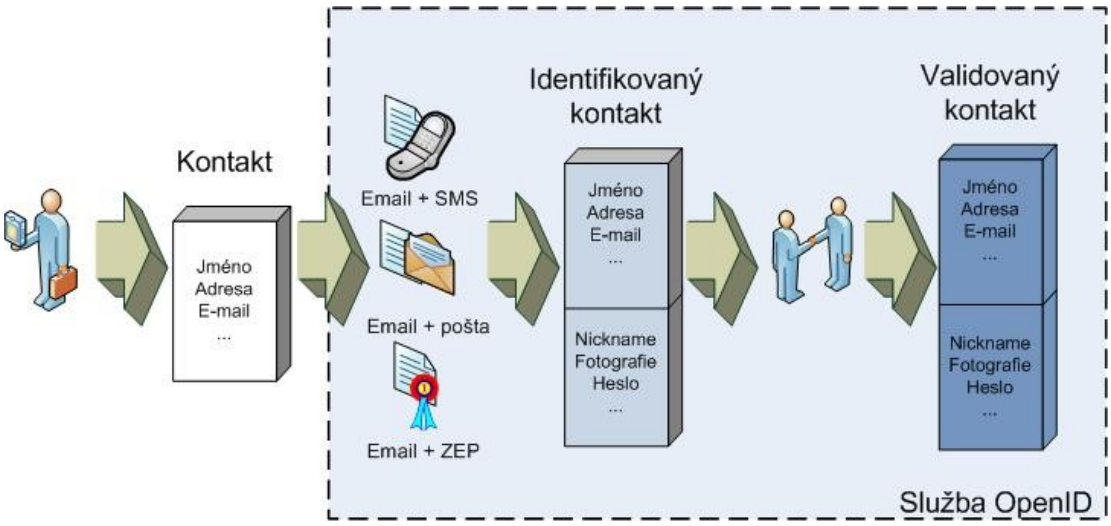
V následujícím seznamu jsou vypsané objekty evidované v centrálního registru, které jsou podstatné pro implementaci systému OpenID.

- **Kontakt** Kontakt je základní objekt systému správy domén reprezentující fyzickou nebo právnickou osobu, která může v centrálním registru vystupovat buď jako držitel domény nebo jako administrátor u domény, nssetu nebo keysetu. Kontakt obsahuje údaje jako jméno, organizaci, adresu, telefon, email a volitelně jeden další identifikační údaj ze skupiny (číslo OP, datum narození, identifikátor MPSV). Kontakty vytvářejí, mění a ruší registrátoři na základě požadavků od uživatelů. Tento (neidentifikovaný) kontakt je dále nazýván běžný kontakt. Odkazovaná osoba je nazývána vlastník kontaktu.
- **Identifikovaný kontakt** Identifikovaný kontakt je takový kontakt, u kterého proběhla základní identifikace vlastníka kontaktu jedním z předepsaných způsobů. Proces identifikace zajistí základní stupeň důvěry v údaje kontaktu. Identifikovaný kontakt získá automaticky heslo pro přihlášení. Detailní informace a proces vytvoření identifikovaného kontaktu je popsán v samostatné kapitole.
- **Validovaný kontakt** Validovaný kontakt je takový identifikovaný kontakt, u kterého je zaručeno, že proběhl proces ověření totožnosti vlastníka kontaktu nazvaný proces validace. Informace, že je kontakt validovaný, je uložena ve speciální položce identifikovaného kontaktu. Postup validace je popsán v samostatné kapitole.

- **Poskytovatel služby** Poskytovatel služby je právnická nebo fyzická osoba, která má zájem používat tento sytém pro autentizaci svých zákazníků. Každý poskytovatel služeb, který požaduje přístupu k údajům identifikovaného kontaktu a má uzavřenou příslušnou smlouvu, bude mít vytvořen objekt v centrálním registru. Kromě evidenčních účelů pak slouží ten objekt jako vazební pro určení jaká data identifikovaných kontaktů budou přístupná tomuto poskytovateli služeb.
- **Požadavek** Do centrálního registru přicházejí od uživatelů požadavky z jednotlivých rozhraní. Každý požadavek je zaevidován spolu s výsledkem. Nově budou do tohoto procesu zahrnuty požadavky na autentizaci z rozhraní pro poskytovatele služeb. S každým požadavkem se ukládají všechny jeho parametry, které do registru vstupují. V případě požadavku na autentizaci se kromě společných záznamů (např. IP adresa uživatele) zaevidují i IP adresa poskytovatele služeb, identifikátor poskytovatele, zadaný identifikátor identity a zvolený způsob autentizace. Nebude se ukládat heslo, které uživatel vyplnil. Evidenci požadavků na autentizaci bude moci vlastník kontaktu prohlížet přes rozhraní pro správu identifikovaného kontaktu.

Identifikovaný kontakt a proces identifikace

Identifikovaný kontakt je kontakt, u kterého byl proveden proces identifikace popsaný níže. Cílem procesu identifikace, je zajistit základní důvěru v údaje kontaktu, u kterých v tuto chvíli neexistuje žádná garance spolehlivosti. Identifikovaný kontakt je možné použít pro autentizaci pomocí protokolu OpenID. Kontakty v centrálním registru, které neprošly procesem identifikace, nemohou být pro službu OpenID použity.



Obr.: Postup identifikace a validace kontaktu

Vztah identifikovaného kontaktu a kontaktu v centrálním registru

Nový kontakt ve stávajícím centrálním registru může vytvořit pouze registrátor. Tento registrátor se pak stává učeným registrátorem kontaktu a pouze on může měnit data tohoto objektu. Registrátor tím přebírá za data zodpovědnost a podle pravidel registrace by měl v přiměřené míře zajistit jejich správnost. Žádný jiný registrátor nemůže měnit data tohoto kontaktu. CZ.NIC může měnit údaje kontaktu, pouze pokud je mu to uloženo na základě soudního rozhodnutí. Pokud chce uživatel zodpovědný za daný objekt měnit data přes jiného registrátora, musí provést transfer objektu k tomuto registrátorovi.

Aby bylo možné existující kontakt v centrálním registru používat pro službu OpenID, musí se nad tímto kontaktem provést identifikace. Tímto procesem přebírá zodpovědnost za data kontaktu CZ.NIC. Takovýto kontakt je ale nadále možné používat pro správu domén.

V rámci procesu identifikace tedy bude proveden standardní transfer od současného registrátora kontaktu a v kolonce Určený registrátor bude nadále uvedeno pouze OpenID. O této operaci bude původní registrátor informován přes EPP rozhraní poll zprávou o transferu. Původní registrátor tak nadále nemá možnost měnit data kontaktu. Registrátor ale k tomuto účelu může uživatele přesměrovat na Rozhraní pro správu identifkovaného kontaktu popsané v samostatné kapitole. Souběžně bude nastaven u kontaktu příznak Transfer prohibited, takže nebude možné automaticky převést kontakt k jinému registrátorovi. Tento příznak zmizí, pokud vlastník kontaktu z vlastní vůle zruší identifikaci kontaktu a tím z něj vytvoří běžný kontakt. Takový kontakt lze pak opět převést k jinému registrátorovi, ale není možné ho využít pro službu OpenID.

Vzhledem k tomu že identifikátor kontaktu je součástí openid identifikátoru, není možné předchozím způsobem převést kontakty, jejichž identifikátor není v přípustném formátu domény (pouze písmena, číslice a pomlčka). Vlastník tohoto kontaktu si musí vytvořit kontakt nový, a pokud ho chce používat místo původního, změnit navázané objekty přes svého registrátora.

Údaje identifikovaného kontaktu

Údaje identifikovaného kontaktu je možné popsat pomocí několika charakteristik:

- **Kategorie** - Každý údaj lze jednoznačně zařadit do následujících kategorií podle jejich významu:
  - **Základní údaje objektu (Object)** - Společná data pro všechny registrovatelné objekty v centrálním registru. Většina těchto údajů nelze přímo nastavit, jsou nastaveny jako důsledek některých operací nad kontaktem.
  - **Základní údaje kontaktu (Contact)** - Zde jsou data společná všem kontaktům v centrálním registru, běžným i identifikovaným.
  - **Autentizační data (Auth)** - Nová skupina údajů sloužící k autentizaci uživatele pomocí OpenID.

    - **Rozšířená data identifikovaného kontaktu (Profile)** - Nová skupina údajů primárně určených pro předání poskytovatelům služeb.
    - **Přístupová práva k datům (Access)** - Nová skupina údajů definující jaká data budou poskytnuta jakým poskytovatelům služeb.
- **Přístup poskytovatele** - Pouze některé z údajů budou předávány poskytovatelům služeb. Poskytovatelé služeb se rozdělují na dva typy – se základním přístupem (označení Base) a s rozšířeným přístupem (označení Advanced). Údaje je možné klasifikovat podle toho pro kterou skupinu poskytovatelů služeb budou předávána
    - **Nepředávané (-)** - Tyto údaje se nikdy nepředávají pro daný typ poskytovatele v rámci protokolu OpenID
    - **Vždy (Always)** - Tyto údaje jsou vždy předávané pro daný typ poskytovatele a není možné jejich předávání zakázat
    - **Volitelně nepředávané (Opt-out)** - U těchto údajů si pro daný typ poskytovatele může uživatel předávání nastavit. Pokud uživatel nestanoví jinak, bude každá vyplněná položka z této kategorie předávána.
    - **Volitelně předávané (Opt-in)** - U těchto údajů si pro daný typ poskytovatele může uživatel předávání nastavit. Pokud uživatel nestanoví jinak, nebude žádná položka z této kategorie předávána.
- **Povinnost** - Některé údaje jsou povinné (Must) a musí být uvedené u každého kontaktu (resp. identifikovaného kontaktu). Ostatní údaje jsou volitelné.

Seznam všech evidovaných údajů identifikovaného kontaktu

Název položky	Kategorie	Přístup pro Base	Přístup pro Advanced	Povinnost
Identifikátor	Object	-	-	Must
Určený registrátor	Object	-	-	Must
Registrátor při vytvoření	Object	-	-	Must
Registrátor při poslední změně	Object	-	-	
Datum a čas posední změny	Object	-	-	
Datum a čas posledního update	Object	-	-	
Datum a čas vytvoření	Object	-	-	Must
Heslo pro transfer	Object	-	-	Must
Jméno	Contact	Opt-out	Opt-out	Must
Organizace	Contact	Opt-out	Opt-out	
Adresa	Contact	Opt-in	Opt-out	Must
Telefon	Contact	Opt-in	Opt-out	

Název položky	Kategorie	Přístup pro Base	Přístup pro Advanced	Povinnost
Fax	Contact	Opt-in	Opt-out	
Email	Contact	Opt-in	Opt-in	Must
Příznaky zveřejnění v WHOIS	Contact	-	-	
Email pro notifikaci o změnách	Contact	-	-	
Daňové identifikační číslo	Contact	Opt-in	Opt-out	
Identifikační řetězec	Contact	Opt-in	Opt-in	
Typ identifikačního řetězce	Contact	Opt-in	Opt-out	
Heslo	Auth	-	-	Must
Certifikát	Auth	-	-	
Mobilní číslo pro OTP	Auth	-	-	
Příznak validace	Profile	-	Always	
Datum narození	Profile	-	-	
Příznak „přes 18“	Profile	Opt-in	Opt-out *	
Přezdívka	Profile	Opt-out	Opt-out	
Obrázek	Profile	Opt-in	Opt-out	
Seznam adres	Profile	Opt-in	Opt-out	
Seznam telefonních čísel	Profile	Opt-in	Opt-out	
Seznam IM identifikátorů	Profile	Opt-in	Opt-out	
Seznam URL	Profile	Opt-in	Opt-out	
Seznam emailů	Profile	Opt-in	Opt-out	
Seznam údajů se změněným přístupem pro skupiny poskytovatelů	Access	-	-	
Seznam údajů se změněným přístupem pro jednotlivé poskytovatele	Access	-	-	
Seznam příslušnosti do skupin pro jednotlivé poskytovatele	Access	-	-	

Příznak „přes 18“ se předává pouze pokud neproběhla validace přes certifikát, v případě validace přes certifikát není datum narození vlastníka kontaktu ověřen.

Proces identifikace

K identifikaci se využívají tyto základní údaje kontaktu: jméno, email, telefon, adresa. Předpokladem je, že telefonní číslo je v mezinárodním formátu a prefix je 420 (Česká Republika) a adresa je z České Republiky (country=CZ). Kontakt může být v centrálním registru již zaregistrován. V takovém případě se nejprve provede operace transfer. Vlastní postup identifikace je následující:

- Uživatel na rozhraní pro správu identifikovaných kontaktů zvolí vytvoření kontaktu nebo převod kontaktu od stávajícího registrátora
    - V případě volby převodu zadá identifikátor kontaktu z centrálního registru
    - V případě volby nového kontaktu vyplní formulář s možností vyplnit všechny údaje kontaktu
- Vygeneruje se náhodné heslo, které se rozdělí na dvě poloviny. Pokud byl zvolen převod kontaktu a nebylo vyplněné heslo pro transfer, bude první polovinu hesla tvořit heslo pro transfer uvedené v centrálním registru doplněné o náhodnou složku. Uživatel si vybere jednu z následujících možností:
    - **Identifikace přes email a telefonní číslo** V případě této volby se první polovina pošle emailem a druhá polovina přes SMS. Jelikož může jít o pevné telefonních číslo, bude se SMS posílat pouze v pracovních hodinách. Zasílání SMS v procesu identifikace bude financovat CZ.NIC.
    - **Identifikace přes email a adresu** V případě této volby se první polovina pošle emailem a druhá polovina poštou na adresu kontaktu. Poštovní služby bude financovat CZ.NIC.
    - **Identifikace s použitím digitálního certifikátu** V případě této volby ověří klientský SSL certifikát. Ten může být libovolného typu od některé z následujících certifikačních autorit (Postsignum, ICA, E-identity) a musí splňovat podmínky že v položkách jméno a email budou stejné údaje jako u kontaktu v centrálním registru. Heslo se potom pošle spojené na email z centrálního registru. Pokud certifikát navíc splňuje podmínky pro validaci (viz. Dále) bude identifikovanému kontaktu rovnou nastaven příznak validace.
- Kontakt se stane identifikovaným v momentu, kdy dojde k prvnímu přihlášení na rozhraní pro správu identifikovaných kontaktů přes spojené heslo.

Není možné provést identifikaci kontaktu, pokud již existuje identifikovaný kontakt se stejným emailem nebo se stejným telefonním číslem nebo u něj byla provedena identifikace se shodným certifikátem a identifikace tohoto druhého kontaktu proběhla před méně než jedním měsícem . V takovém případě identifikace selže už při zadávání údajů (resp. transferu).

V systému bude existovat mechanismus jak zabezpečit všechny zmiňované druhy komunikace (email, telefon, pošta) proti nevyžádaným zprávám.

Uživatel může přes rozhraní pro správu identifikovaných kontaktů změnit kterýkoliv ze svých údajů. Žádná změna těchto údajů nemá vliv na identifikaci a není nutné tento proces po změně opakovat. Některé změny mají ale následující omezení:

- Email a telefonní číslo lze změnit pouze jednou za dva měsíce
- Změnu emailu je nutné potvrdit heslem zaslaným na nový email
- Změnu telefonního čísla je nutné potvrdit heslem zaslaným na toto nové číslo

Identifikovaný kontakt je možné přes rozhraní pro správu identifikovaných kontaktů převést zpět na běžný kontakt a tím se všechny údaje objektu z kategorií Auth, Profile a Access smažou. Pokud nedojde u identifikovaného kontaktu k přihlášení přes nějakého poskytovatele služeb během jednoho roku, zruší se jeho identifikace automaticky a kontakt zůstane nadále jako běžný kontakt. Pro jeho znovupoužití bude třeba proces identifikace zopakovat. Měsíc před zrušením identifikace dostane uživatel na email informaci, že jeho identifikovaný kontakt bude převeden do neidentifikovaného stavu a má možnost toto zrušení odložit přihlášením se na rozhraní pro správu identifikovaných kontaktů.

Validovaný kontakt a proces validace

Validovaný kontakt je takový identifikovaný kontakt, který prošel procesem ověření totožnosti vlastníka kontaktu, nazvaném proces validace. Proces validace má za cíl zajistit, že v centrálním registru je dostatek informací, které umožní jednoznačnou identifikaci vlastníka kontaktu pro případ, že s využitím jeho identity bude zjištěno nějaké nekalé jednání. Úspěšný výsledek procesu validace je uložen v údajích identifikovaného kontaktu v podobě příznaku. Dokumenty obdržené v procesu validace budou archivovány (to se netýká identifikačních dokumentů, např. občanský průkaz, jejichž kopie nebudou pořizovány ani archivovány).

Způsoby validace pro osobní identifikovaný kontakt

- **Pomocí dopisu opatřeného úředně ověřeným podpisem** Pokud správce OpenID obdrží dopis obsahující identifikátor kontaktu a zároveň jméno, datum narození a adresa u tohoto kontaktu v registru odpovídá jménu a adrese v doložce o úředním ověření podpisu, je možné kontakt s tímto identifikátorem prohlásit za validovaný.
- **Osobní návštěvou** Pokud ke správci OpenID přijde uživatel, prokáže se občanským průkazem nebo cestovním dokladem a údaje jméno, datum narození a adresa v registru pro identifikátor, který uživatel poskytne, budou odpovídat údajům v dokladu, je možné kontakt s tímto identifikátorem prohlásit za validovaný.
- **Pomocí SMIME emailu opatřeného digitálním certifikátem** Pokud správci OpenID přijde na emailovou adresu (SMTP/SMIME protokol) žádost o validaci obsahující identifikátor kontaktu a prohlášení, že údaje tohoto kontaktu jsou v souladu se skutečností, tento certifikát je platný (expirace, CLR) obsahuje údaje, které odpovídají údajům v žádosti a byl vydán jako kvalifikovaný certifikát certifikační autoritou akreditovanou v ČR (Postsignum, E-identity, ICA), je možné kontakt s tímto identifikátorem prohlásit za validovaný.

Způsoby validace pro identifikovaný kontakt právnické osoby

- **Pomocí dopisu opatřeného úředně ověřeným podpisem** Pokud správce OpenID obdrží dopis obsahující identifikátor kontaktu a zároveň jméno a adresa u tohoto kontaktu v registru odpovídá jménu a adrese v doložce o úředním ověření podpisu, je možné kontakt s tímto identifikátorem prohlásit za validovaný. Obsahem dopisu musí být také osvědčení skutečnosti, že daná osoba je oprávněna jednat za danou právnickou osobu na základě výpisu z evidence, ve které je právnická osoba zapsána, či potvrzení, že daná osoba je zaměstnancem uvedené právnické osoby, které musí být podepsáno osobou, která je oprávněna za právnickou osobu jednat základě výpisu z evidence, ve které je právnická osoba zapsána. Je-li příslušná osoba zastoupena, musí být k dopisu doložena i plná moc s úředně ověřeným podpisem. Výpis z evidence, ve které je právnická osoba zapsána, jakož i plná moc, nesmí být starší než tři měsíce.
- **Osobní návštěvou** Pokud k registrátorovi přijde uživatel, prokáže se občanským průkazem nebo cestovním dokladem a údaje jméno a adresa v registru pro identifikátor, který uživatel poskytne, budou odpovídat údajům v dokladu, je možné kontakt s tímto identifikátorem prohlásit za validovaný. Součástí žádosti musí být také osvědčení skutečnosti, že daná osoba je oprávněna jednat za danou právnickou osobu na základě výpisu z evidence, ve které je právnická osoba zapsána, či potvrzení, že daná osoba je zaměstnancem uvedené právnické osoby, které musí být podepsáno osobou, která je oprávněna za právnickou osobu jednat základě výpisu z evidence, ve které je právnická osoba zapsána. Je-li příslušná osoba zastoupena, musí být k žádosti doložena i plná moc s úředně ověřeným podpisem. Výpis z evidence, ve které je právnická osoba zapsána, jakož i plná moc, nesmí být starší než tři měsíce.
- **Pomocí SMIME emailu opatřeného digitálním certifikátem** Pokud správci OpenID přijde na emailovou adresu (SMTP/SMIME protokol) žádost obsahující identifikátor kontaktu a prohlášení, že údaje tohoto kontaktu jsou v souladu se skutečností, tento certifikát je platný (expirace, CLR) obsahuje údaje, které odpovídají údajům v žádosti a byl vydán jako kvalifikovaný certifikát certifikační autoritou akreditovanou v ČR (Postsignum, E-identity, ICA), je možné kontakt s tímto identifikátorem prohlásit za validovaný.

Je-li předkládána jakákoliv listina s úředním ověřením pravosti listiny nebo podpisu jednající osoby a toto ověření provádí zahraniční subjekt, musí být provedeno vyšší ověření dané listiny (tzv. superlegalizace) dle zákona o mezinárodním právu soukromém a procesním. Superlegalizaci nahrazuje apostillační doložka dle Úmluvy o zrušení požadavku ověřování cizích veřejných listin ze dne 5. 10. 1961, popřípadě postup stanovený příslušnou dvoustrannou mezinárodní smlouvou, v souladu s níž je daná listina osvobozena od vyššího ověření. Je-li předkládána jakákoliv listina v jiném než českém, slovenském nebo anglickém jazyce, musí být k listině přiložen úředně ověřený překlad listiny do jednoho z těchto jazyků včetně případných ověřovacích doložek. Zajištění těchto formálních náležitostí je povinností osoby, která předkládá danou listinu.

Po nastavení příznaku validace má jakákoliv změna údajů v registru (jméno, organizace a adresa) za následek zrušení příznaku validace. Ostatní údaje kontaktu je možné měnit libovolně bez zrušení tohoto příznaku.

Evidence poskytovatelů a nastavení přístupu poskytovatelů k datům kontaktu

Poskytovatelé služeb komunikují s centrálním registrem přes specializované rozhraní protokolem OpenID. V rámci komunikace dochází k výměně informací o úspěšné nebo neúspěšné autentizaci uživatele a k přenosu dat uvedených v centrálním registru u příslušného identifikovaného kontaktu. Z hlediska možností, které centrální registr poskytovatelům služeb nabízí se tito rozdělují na dvě kategorie:

- **Poskytovatelé se základním přístupem** Sem spadají všichni poskytovatelé, kteří přistupují k centrálnímu registru protokolem OpenID a nemají podepsanou smlouvu o přístupu k datům. Těmto poskytovatelům se po úspěšném přihlášení nabídne z údajů identifikovaného kontaktu pouze jméno, organizace, email a nickname. Uživatel si bude moci u svého kontaktu seznam poskytnutých údajů rozšířit nebo zúžit. Tento přístup bude zdarma.
- **Poskytovatelé s rozšířeným přístupem** Pokud chce poskytovatel získat více informací o uživateli, musí podepsat příslušnou smlouvu. Základní sada údajů, které se mu v takovém případě poskytnou, se rozšíří na kontaktní informace (email, telefon a adresa) a příznak validace. Uživatel si opět bude moci u svého kontaktu seznam poskytnutých údajů rozšířit nebo zúžit. Příznak validace bude posílán vždy. Pro tyto poskytovatele bude v systému existovat evidence. Tento přístup bude zpoplatněný podle zvláštního ceníku.

Komunikace s rozhraním pro poskytovatele služeb bude mít následující vlastnosti:

- Poskytovatel zahajuje na pozadí komunikaci otevřením HTTPS komunikace na OpenID rozhraní. Podle klientského certifikátu se ověří, zda jde o poskytovatele se základním nebo rozšířeným přístupem.
- Poskytovatel přesměruje uživatele na OpenID rozhraní. Součástí požadavku jsou následující informace:
    - Identifikátor uživatele, který se autentizuje
    - Identifikátor poskytovatele
    - Požadavek na typ autentizace. Pokud tento požadavek chybí, bude si moci uživatel vybrat ze všech možností, které má nastavené. Pokud požadovaný typ nemá uživatel nastaven, bude mít možnost přejít na stránky rozhraní pro správu identifikovaných kontaktů a tam si tyto údaje nastavit. V případě, že této možnosti nevyužije, požadavek selže.

V evidenci v centrálním registru bude u každého poskytovatele služeb s rozšířeným přístupem uvedeno následující:

- Identifikátor poskytovatele - Jednoznačný identifikátor, který posílá poskytovatel v rámci přesměrování autentizačního požadavku. V protokolu OpenID tomuto identifikátoru odpovídá položka "realm"
- Název poskytovatele - Název organizace z obchodního rejstříku (nebo jméno v případě fyzické osoby) bude odpovídat údaji na smlouvě.
- Adresa poskytovatele - Adresa sídla, bude odpovídat údaji na smlouvě.
- Identifikátor kontaktu - Podrobnější údaje o poskytovateli služeb (email, telefon...) budou převzaty z odkazovaného kontaktu v centrálním registru a sám poskytovatel služeb si může tyto údaje udržovat aktuální. Název organizace a adresa sídla je uvedena zvlášť aby nemohlo dojít k jejímu přepsání bez změny smlouvy.
- SSL Certifikát - Pro autentizaci tohoto poskytovatele v rámci HTTPS komunikace s OpenID rozhraním.
- Soubor s logem poskytovatele zobrazené v rozhraní pro veřejnost.
- URL pro přesměrování na systém poskytovatele služeb zobrazené v rozhraní pro veřejnost.

Po úspěšné autentizace uživatele dojde k předání některých údajů identifikovaného kontaktu z centrálního registru do systému poskytovatele služeb. Jak je popsáno v kapitole o údajích identifikovaného kontaktu, jsou některé údaje předávaný vždy a některé údaje volitelně. Seznamy definující přístupy poskytovatelů služeb k těmto volitelně předávaným údajům jsou samy součástí údajů identifikovaného kontaktu. Pro jednodušší nastavení přístupu si může uživatel nadefinovat skupiny poskytovatelů a nastavit těmto skupinám práva pro předávání údajů identifikovaného kontaktu.

Poskytovatelé služeb nemohou žádným způsobem měnit data v centrálním registru. Pro potřeby případné synchronizace mohou poskytovatelé služeb využít rozhraní pro aktualizaci údajů popsané v samostatné kapitole. Adresa tohoto rozhraní bude součástí předávaných dat po úspěšné autentizaci.

Mazání kontaktů z důvodu nepoužívání

Pokud je kontakt zároveň OpenID identitou, bere se jako by byl navázán na jiný objekt v centrálním registru a nebude odregistrován po šesti měsících nepoužívání. Teprve pokud dojde ke zrušení identifikace kontaktu, začíná běžet šestiměsíční lhůta. Pokud nedojde ke změně údajů kontaktu, k navázání kontaktu na jiný objekt centrálního registru nebo ke znovuvytvoření identifikovaného kontaktu, bude tento kontakt smazán.

Rozhraní pro veřejnost

Centrální registr zveřejňuje některá data přes rozhraní pro veřejnost. V následující kapitole budou popsány jednotlivé moduly veřejného rozhraní centrálního registru a jeho změny v souvislosti s OpenID.

Unixový whois

Prostřednictvím standardního unixového protokolu whois může veřejnost zjišťovat informace o všech registrovatelných objektech centrálního registru (kontakty, domény, nssety a keysety) a o jejich registrátorech. Objekty jsou vyhledávány podle jejich identifikátoru, který je jednoznačný v rámci typu objektu. Pokud je objekt zaregistrován, vrátí se buď jen informace o tomto objektu, nebo navíc informace o všech navázaných objektech. Služba umožňuje také některé druhy reversního vyhledávání (např. všechy domény nějakého kontaktu). Počet zobrazených objektů je limitován. V detailu kontaktu je možno uživatelem některé údaje zablokovat proti zveřejnění přes službu whois. Přístup ke službě je zabezpečen proti robotům detekcí vícenásobných přístupů z konkrétní IP adresy.

Identifikované kontaky jakožto rozšíření kontaktů jsou také objektem zveřejňovaným službou whois. Toto zveřejňováni má navíc dvě následující pravidla:

1. Nebude zveřejněn žádný z rozšiřujících údajů kontaktů (kategorie Auth, Profile a Access).
2. Pokud libovolný kontakt (běžný i identifikovaný) není navázán na žádný jiný objekt v centrálním registru, dotaz na identifikátor takového kontaktu pouze zobrazí, že identifikátor je registrován.

Webový whois

Webová služba whois je alternativou ke klasickému unixovému whoisu integrovanou do webové prezentace CZ.NIC. Oproti klasické unixové službě whois obsahuje více detailů o jednotlivých objektech a využívá hypertextových odkazů pro přechod mezi detailu navázaných objektů. Webová verze whois neumožňuje reverzní prohledávání. Přístup je službě je zabezpečen proti robotům kombinací detekce IP adres a technologie CAPTCHA. Změny v souvislosti s identifikovaným kontaktem popsané u klasického unixového whoisu platí i pro webovou variantu.

Žádosti do registru

Přestože veškeré změny nad objekty centrálního registru prováději uživatelé přes určené registrátory, existuje několik situací, ve kterých mohou kontaktovat přímo registr. Pro žádosti uživatelů do registru slouží zvláštní webové stránky. Autentizace žádostí je prováděna buď digitálním podpisem anebo notářsky ověřeným podpisem. Tímto způsobem lze zažádat zaslání hesla k transferu (authinfo) nebo o zablokování/odblokování transferu nebo všech změn nějakého objektu.

Z pohledu služby OpenID dochází ke změně v interpretaci žádosti o odblokování transferu. Vzhledem k tomu, že identifikovaný kontakt není možné převádět, nebude tato žádost v tomto případě akceptována.

Seznam poskytovatelů služeb s rozšířeným přístupem

Nově bude stránkách CZ.NIC věnovaných OpenID zobrazen seznam poskytovatelů s rozšířeným přístupem. Tento seznam bude obsahovat:

- Logo organizace
- Název organizace
- URL odkazující na systém poskytovatele služeb

Statistiky

Na stránkách CZ. NIC jsou k dispozici některé statistiky z provozu registru. Tyto veřejné statistiky budou rozšířeny o počet identifikovaných a validovaných kontaktů.

Rozhraní pro poskytovatele služeb

Klíčovou komponentou služby OpenID je tento nový typ rozhraní do centrálního registru. Toto rozhraní je určeno pro poskytovatele služeb, kteří jej využijí pro přesměrování procesu autentizace jejich uživatelů pomocí technologie OpenID. Každý požadavek na tomto rozhraní bude zalogován. Komunikace na tomto rozhraní je přesně popsána ve specifikacích OpenID Authentication 2.0, OpenID Attribute Exchange 1.0 a OpenID Provider Authentication Policy Extension 1.0.

Pro přihlášení u poskytovatele služeb může uživatel použít buď openid identifikátor vzniklý spojením identifikátoru kontaktu v centrálním registru a domény id.nic.cz nebo přímo identifikátor správce OpenID id.nic.cz. Ve druhém případě musí vyplnit identifikátor kontaktu v centrálním registru v přihlašovacím formuláři. Požadavek na autentizaci od poskytovatele služeb může volitelně obsahovat preferovanou metodu autentizace z podporovaných možností. Pokud tato preference není uvedena, bude si moci zvolit tuto metodu sám uživatel.

V rámci každého přihlášení se vytvoří v systému session, která bude svázaná přes mechanismus cookies s prohlížečem uživatele. Pokud je tato session aktivní a požadavek na autentizaci přijde od poskytovatele služeb, který je v údajích identifikovaného kontaktu označen jako důvěryhodný, dojde k automatickému úspěšnému vyřízení tohoto požadavku.

Viditelnou částí autentizačního rozhraní bude webová stránka, která bude sloužit ke vložení doplňujících údajů pro provedení autentizace – OpenID identifikátor bude předán už z aplikace poskytovatele služby. Stránka bude obsahovat:

- Identifikátor poskytovatele služby, který žádá o autentizaci.
- OpenID identifikátor pokud je součástí požadavku nebo volbu identifikátoru pokud není
- Volbu typu autentizace (výběr z menu)
- Pole na vyplnění autentizačního údaje (editovatelné pole, které se zobrazí dle typu autentizace)
- Tlačítko na odeslání

Metody autentizace jsou následující:

- **Autentizace heslem** Každý identifikovaný kontakt má heslo, které obdrží v rámci procesu identifikace a může si ho změnit přes Rozhraní pro správu identifikovaných kontaktů. Autentizace je úspěšná, pokud zadané heslo souhlasí s heslem uvedeným u identifikovaného kontaktu.
- **Autentizace certifikátem** U identifikovaného kontaktu je možné uložit certifikát ve formátu x509. Při volbě této metody bude provedena SSL autentizace a porovnán SSL klientský certifikát. Pokud tento certifikát odpovídá certifikátu uloženému u identifikovanému kontaktu je autentizace úspěšná.
- **Autentizace jednorázovým heslem (OTP)** Při volbě této metody bude vygenerováno heslo a zasláno na mobilní číslo uložené v příslušném údaji identifikovaného kontaktu. Autentizace bude úspěšná, pokud se tento kontakt přihlásí do 5 minut tímto heslem. Zasílání těchto SMS bude zpoplatněno systémem PremiumSMS.

Systém bude rozšiřitelný o další případné metody autentizace podle zájmu uživatelů.

Po odeslání přihlašovací stránky bude provedena autentizace uživatele a její výsledek bude uživateli zobrazen. V případě, že autentizace proběhne úspěšně, bude uživateli zobrazena informace o tom, že bude přesměrován zpět na stránky poskytovatele služby a bude mu nabídnut seznam údajů o jeho identifikovaném kontaktu, které se tomuto poskytovateli předají .. Pokud s předáním těchto údajů nesouhlasí, bude mít možnost přihlášení stornovat. Toto platí pouze v případě že se jedná o uživateli dosud neznámého poskytovatele služeb. Uživatel bude mít možnost přejít v takovém případě do prostředí Rozhraní pro správu identifikovaných kontaktů a tomuto poskytovateli přidělit jiná pravidla pro předávání údajů. Pokud se ale jedná o poskytovatele služeb, který je v uživatelově seznamu známých poskytovatelů s nadefinovaným seznamem předávaných údajů, proběhne přesměrování bez nutnosti cokoliv potvrzovat. V případě, že autentizace selže (např. z důvodu špatného hesla), bude nabídnuta uživateli přihlašovací obrazovka ještě 2x, aby mohl autentizaci zopakovat. Pokud ani další dvě autentizace nebudou úspěšné, bude uživatel informován o definitivně neúspěšné autentizaci a bude také přesměrován zpět na stránky poskytovatele služby. .

Součástí systému bude i ukázková aplikace, která bude k dispozici poskytovatelům služeb, kteří budou chtít podporovat OpenID ve svých aplikacích. Tato aplikace bude implementovat celý tento autentizační proces. Aplikace bude napsaná jako moduly v několika jazycích, které bude možné jednoduše integrovat do webových systémů poskytovatelů.

Rozhraní pro správu identifikovaných kontaktů

Toto rozhraní mohou využívat uživatelé vlastnící nějaký identifikovaný kontakt ke správě svých údajů případně k identifikaci základního kontaktu již existujícího v centrálního registru. Jedná se o webovou aplikaci dostupnou na webu CZ. NIC, která se bude pro potřeby autentizace chovat jako poskytovatel služeb a bude využívat autentizační rozhraní pro poskytovatele služeb.

Webová aplikace bude umožňovat práci ve dvou základních režimech:

1. Nepřihlášený uživatel. V tomto režimu má každý uživatel k dispozici následující dvě funkce (obě funkce budou chráněny mechanismem Captcha proti robotům):
    - Žádost o transfer kontaktu k CZ.NIC OpenID registrátorovi. Uživatel bude dotázán na identifikátor kontaktu a heslo pro transfer. Poté dojde k pokusu o transfer objektu. O výsledku bude uživatel okamžitě informován.
    - Žádost o identifikaci kontaktu. Uživatel bude dotázán na identifikátor kontaktu a na metodu identifikace jak je uvedeno v kapitole o identifikaci kontaktu. Pokud identifikace proběhne úspěšně, má uživatel heslo, které může začít používat v rámci technologie OpenID a zároveň se tímto heslem může autentizovat pro přístup do režimu přihlášeného uživatele této aplikace
2. Přihlášený uživatel. V tomto režimu má uživatel možnost pomocí webového editoru změnit jakýkoliv údaj u svého identifikovaného kontaktu. Aplikace bude změny uživatele online zasílat do centrálního registru. V tomto režimu bude moci také uživatel požádat o validaci svých dat. Na základě vybrané metody bude tato žádost vyřízena okamžitě nebo o jejím výsledku bude posléze uživatel informován emailem na adresu z centrálního registru. Uživatel bude moci také procházet historii předchozích autentizací.

Údaje o jednotlivých autentizacích (přístupech uživatele na službu OpenID) budou archivovány po dobu 6 měsíců. Uživatel bude mít možnost prohledávat historii vlastních přístupů a také možnost nastavit prodloužení lhůty archivace jeho logů, a to až na období 2 let (s přednastavenou granularitou).

CZ.NIC je oprávněn poskytnout takto archivované údaje orgánům státní správy a soudů, včetně rozhodčího soudu, a to v souladu se zákonem a v rámci jejich úřední činnosti nebo v rámci rozhodování sporů. Takto lze poskytnout pouze údaje vztahující se ke konkrétním kontaktům. Takto archivované údaje nebudou poskytovány jednotlivým poskytovatelům služeb.

Technické řešení služby OpenID

Základní vlastnosti

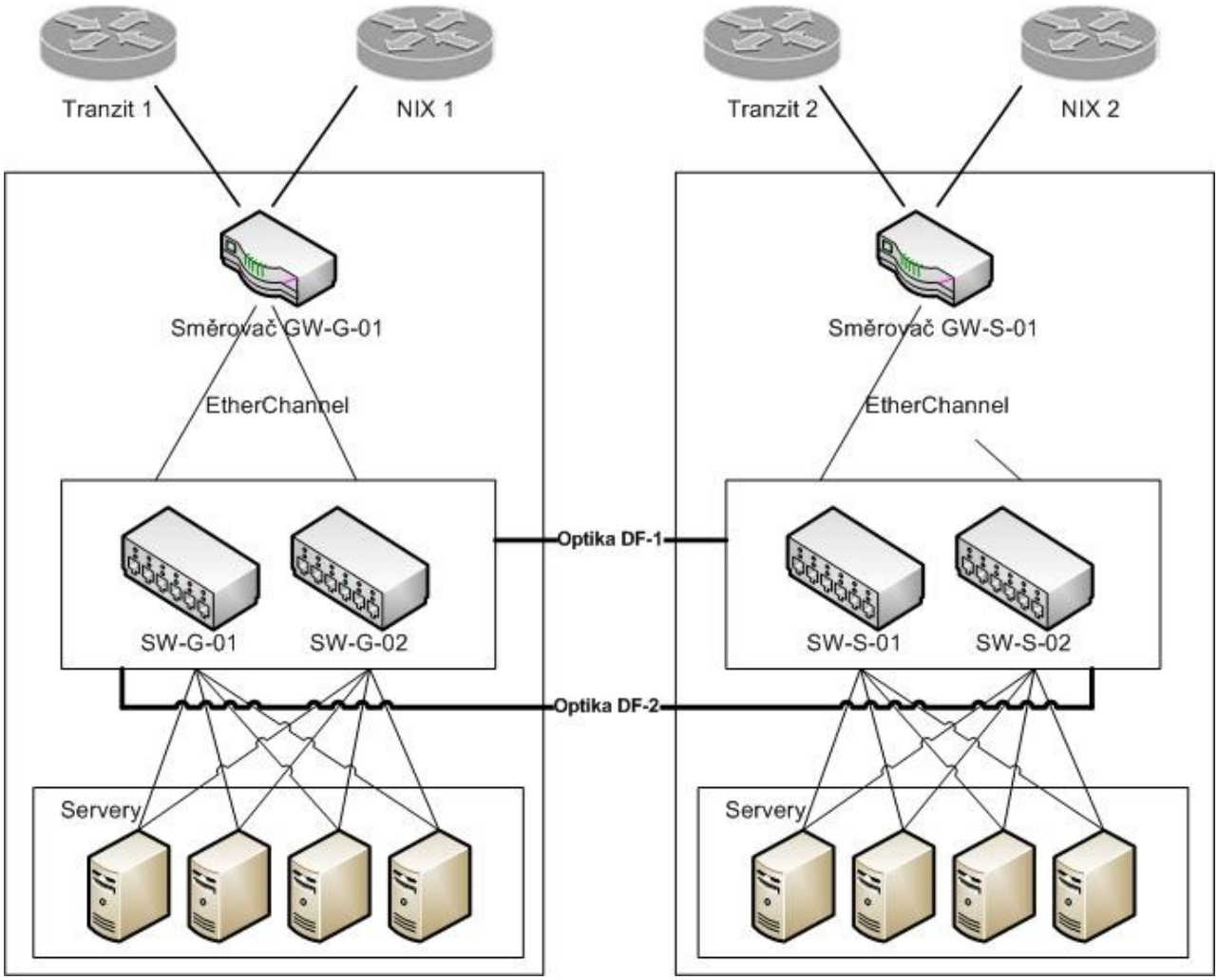
Registr OpenID je koncipován jako rozšíření stávajícího centrálního registru DSD-NG. Na základě tohoto faktu bude u komponent, které nelze vydělit mimo stávající systém centrálního registru DSD-NG, využit hardware a systémový software. Jedná se především o databázový server a diskové pole pro databázový server.

Registr OpenID je postaven komponentově a jednotlivé komponenty budou naprogramovány tak, aby bylo možné je provozovat na samostatných oddělených serverech. Všechny komponenty bude v maximální možné míře spustit a paralelně provozovat ve více instancích pro zajištění dostatečného výkonu s výhledem na masivnější rozšíření služby OpenID mezi uživateli. Komponenty, které z provozního hlediska není možné provozovat ve více instancích, budou provozovány v režimu hot-standby. Především se jedná o databázový server, kde budou data replikována na záložní server a v případě selhání primárního serveru bude možné poruchu odstranit v krátkém čase díky použití repliky.

Geograficky oddělené lokality

Registr OpenID bude provozován stejně jako centrální doménový registr DSD-NG v minimálně dvou nezávislých geograficky oddělených lokalitách. Každá lokalita bude schopna samostatného provozu systému OpenID, tak aby se zamezilo výpadkům služby OpenID, a byl zajištěn nepřetržitý provoz. Autentizační komponenta umožňující přihlášení uživatelů pomocí OpenID autentizačního protokolu bude zajištěna dalšími mechanismy pro zvýšení její spolehlivosti. Případná terciální záložní lokalita bude vybudována mimo Prahu. Vše viz následující obrázek.

Umístění jednotlivých lokalit bude zvoleno tak, aby vybraný telehouse poskytoval zálohované napájení včetně dieselových generátorů, dostatečnou zálohovanou chladící kapacitu, a také vhodné propojení do peeringových center a široký výběr poskytovatelů tranzitního připojení (viz. níže oddíl o síťové infrastruktuře).

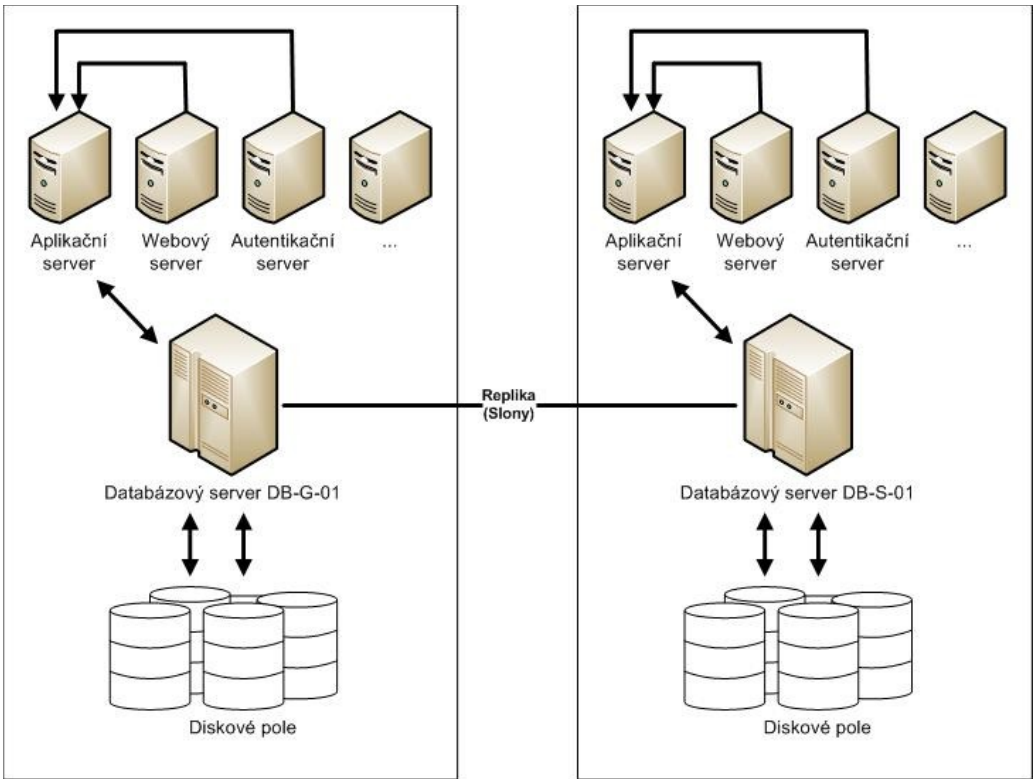


Obr.: Rozdělení systému do geograficky oddělených lokalit

Hardware

Každá komponenta bude provozována na minimálně dvou serverech. Dodavatelé serverů a jednotlivé součásti serverů (architektura CPU, atd.) budou vybrány tak, aby byla vyloučena homogenita použitého hardware. Použitý operační systém bude Linux, který bude pro zvýšení heterogenity prostředí provozován ve variantě i386 a amd64. Tímto bude minimalizována možnost celkového selhání vadou hardware, či externím útokem využívající konkrétní chybu v architektuře HW či SW. Dodavatelé serverových komponent budou vybráni s ohledem na jejich spolehlivost a stabilitu pro zajištění kontinuity. Současný systém DSD-NG používá jako dodavatele společnosti HP a Dell, které k serverům poskytují záruku NBD. Jednotlivé komponenty serverové platformy budou vybírány také dle jejich podpory v operačním systému Linux. Všechny servery mají redundantní napájení do dvou nezávislých napájecích větví od provozovatele telehouse.

Použitá disková pole jsou také od dvou nezávislých dodavatelů. S výhledem do budoucna je také možné uvažovat o vybudování nezávislé FiberChannel sítě a replikaci dat na úrovni diskových polí se zachováním stávající replikace na databázové úrovni. Tímto bude zajištěno zálohování dat na několika úrovních.



Obr.: Rozdělení systému do komponent

Síťová infrastruktura

Pro připojení registru OpenID do sítě Internet bude využita stávající síťová infrastruktura, která je vybudována na dvou nezávislých platformách – Cisco a Juniper. Všechny propojení mezi jednotlivými částmi síťové infrastruktury včetně připojení serverů je realizováno dvěma fyzicky nezávislými propoji, z nich každý je připojen do jiného přepínače. Tyto dva propoje jsou spojeny do jednoho virtuálního kanálu pomocí technologie EtherChannel (na linuxu se tato technologie nazývá interface bonding). Přepínače v lokalitách jsou propojeny do tzv. stacku, kdy je několik přepínačů navzájem propojeno do jednoho logického bloku a výpadek jednotlivého přepínače je vyřešen převzetím provozu pomocí dalšího přepínače ve stacku. Tímto je zajištěna dostupnost serverů a směrovačů i v případě kompletního selhání jednoho z přepínačů. Stejným způsobem jsou redundantně propojeny jednotlivé geograficky nezávislé lokality. Každý z přepínačů i směrovačů je zapojen do dvou nezávislých elektrických větví.

Připojení do sítě Internet bude realizováno pomocí minimálně dvou nezávislých poskytovatelů tranzitní konektivity a dvou nezávislých propojů do peeringového centra NIX.CZ (případně do jiných významných peeringových center). Každá geograficky oddělená lokalita bude disponovat minimálně jedním propojem k poskytovateli tranzitní konektivity a jedním propojem do peeringového centra. Směrovače jsou navzájem propojeny pomocí protokolu BGP (iBGP), tudíž v případě výpadku peeringového centra nebo poskytovatele tranzitní konektivity v jedné z lokalit neznamená výpadek této lokality, ale pouze přesměrování IP provozu do další lokality.

Obě hlavní lokality (primární a sekundární) jsou navzájem propojeny pomocí nenasvícených optických vláken. Propoj je redundantní a optická vlákna jsou vedena dvěma nezávislými trasami, aby byla zajištěna odolnost proti přerušení optických vláken. Lokality jsou propojeny na L2 vrstvě mezi přepínači a opět je zajištěna odolnost proti výpadku pomocí technologie EtherChannel a stackováním přepínačů.

Zálohování

Zálohování dat systému DSD-NG a OpenID je prováděno pomocí skriptů vyvinutých pro potřeby centrálního registru. Zálohování se provádí jednou denně v nočních hodinách. Technologie zálohování z důvodů rychlosti a spolehlivosti využívá standardních disků v zálohovacím serveru, který je umístěn v jiné lokalitě než primární databázový server. Zálohovací skripty využívají standardní GNU nástroje na zálohování (TAR, GZIP, BZIP2), případně nástroje určené k zálohování aplikací (např. pg_dump pro databázi PostgreSQL).