

Autentifikácia v D2000

Autentifikáciou sa rozumie overenie identity užívateľa, t.j. overenie, že užívateľ je ten, ktorý tvrdí, že je. Overenie identity obecné prebieha na základe nieho, o užívateľa vie (prihlasovacie meno + heslo), o vlastní (prihlasovací USB token, osobná IPová karta so šifrovaním a identifikaným kúrom PKI), prípadne nejakého jeho merateľného biometrického znaku (odtlačok prsta, scan dúhovky). Štandardne overuje meno a heslo užívateľa v D2000 proces [D2000 Server](#). V niektorých prípadoch je výhodné, aby overovanie identity užívateľa bolo presunuté na doménu Windows, o možnosti:

- používanie tých istých hesiel do D2000 ako do Windows domény ([NTLM autentifikácia](#)),
- používanie tých istých mien a hesiel do viacerých systémov D2000, pre ich zmenu stačí zmeniť heslo na jednom mieste - heslo do Windows ([NTLM autentifikácia](#)),
- automatické prihlásenie sa do D2000 bez zadávania mena a hesla iba na základe toho, že užívateľ je prihlásený do Windows domény ([Kerberos autentifikácia](#)),
- zabezpečí prihlásenie užívateľa do D2000 hardvérovou (prihlasovací USB token, osobná IPová karta so šifrovaním a identifikaným kúrom PKI) tak, že sa takéto zabezpečenie použije na prihlasovanie sa užívateľa do Windows a následne sa použije [Kerberos autentifikácia](#) na prihlásenie do D2000,
- zakázanie prihlásenia užívateľa do D2000 nástrojmi pre správu užívateľov v doméne Windows,
- nastavenie parametrov, ktoré musí spať heslo do D2000, nástrojmi pre správu užívateľov v doméne Windows.

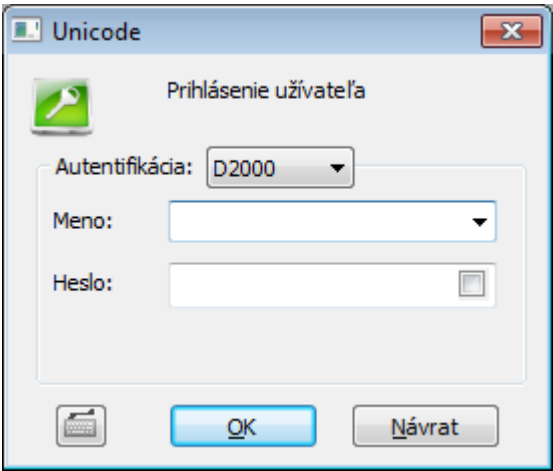
Poznámka pre platformy Linux a Raspberry PI: od verzie D2000 12.2.65 (patche z 27.5.2020 a novšie) je [Kerberos autentifikácia](#) dostupná aj na platformách Linux x64 a Raspberry PI. Na sfunkčnenie je nutné vykonať nasledovné kroky:

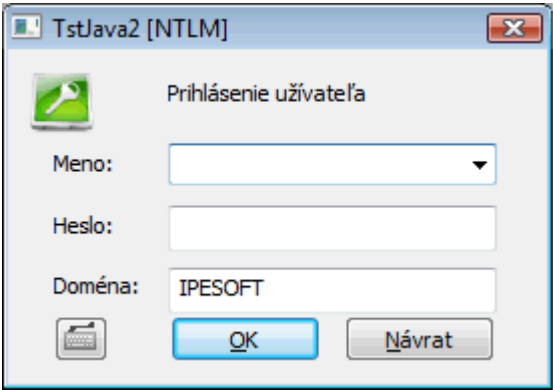
- zaradenie Linux/Raspberry PI servera do Windows domény (príkazom `realm join meno_domény`, napr. `realm join IPSTEST.SK`)
- umožnenie prístupu D2000 Serveru (*kernel*) k súboru `/etc/krb5.keytab`. Jednou možnosťou je nakonfigurovať spúšťanie D2000 Servera pod užívateľom `root`, inou - menej dramatickou - je nakonfigurovanie prístupových práv pre skupinu, pod ktorou je spustený D2000 Server. Napríklad ak je použitá skupina `d2users`, tak treba spustiť:
`chgrp d2users /etc/krb5.keytab`
`chmod 640 /etc/krb5.keytab`

Na platforme Linux bola otestovaná autentifikácia v rámci jednej domény (*IPSTEST.SK*) aj medzi dvoma doménami (*hi.exe* spustené pod užívateľom v doméne *IPESOFTE.SK*, D2000 server na Linuxovom serveri v doméne *IPSTEST.SK*). V oboch prípadoch bola hodnota parametra [AuthSecPrinc](#) nastavená na `SRVAPP$@IPSTEST.SK`, kde *SRVAPP* je názov linuxového počítača zaradeného do Windows domény.

Metódy autentifikácie

V systéme D2000 sú podporované nasledovné metódy autentifikácie:

Metóda autentifikácie	Popis
D2000	<p>Overovanie užívateľského mena a hesla procesom D2000 Server. Toto je štandardná metóda autentifikácie, ktorá využíva meno a heslo uložené v konfigurácii objektu Užívateľ. Prihlasovací dialóg zobrazuje užívateľské meno a heslo:</p> 

NTLM	<p>Overovanie mena a hesla zadaného užívateľom vykonáva autentifikovaný subsystém Windows NTLM (NT LAN Manager) dostupný od verzie Windows NT 4.0, pričom sa autentifikácia vykonáva v doméne, ktorú udáva konfigurovaný parameter užívateľa Doména. D2000 Server získa po dokončení autentifikácie od Windows informáciu o úspešnom/neúspešnom overení užívateľského mena a hesla v doméne. Pokiaľ bola autentifikácia úspešná, poda užívateľského mena vyhľadá objekt typu Užívateľ a skontroluje, či má užívateľ nakonfigurovanú autentifikáciu metódou NTLM ako povolenú (parameter Metódy autentifikácie), či je zhodný názov domény a či nemá za kázané prihlásenie.</p> <p>Prihlasovací dialóg zobrazuje užívateľské meno a heslo, v záhlaví má okrem názvu aplikácie aj text <i>[NTLM]</i> a pod menom a heslom doménu, do ktorej sa užívateľ prihlasuje:</p>  <p>Poznámka: NTLM autentifikácia je použitá na samostatnom počítači s lokálne definovanými užívateľmi (vtedy Doména je názov počítača) ako aj vo Windows doméne (Doména je názov domény). Ak nie je možné kontaktovať autentifikáciu autoritu, prihlásenie neprebehne. Prihlasovanie sa zmení na autentifikáciu podľa D2000 a užívateľovi sa zobrazí upozornenie "Neúspešná NTLM autentifikácia. Zadájte prihlasovacie meno a heslo z D2000."</p>
Kerberos	<p>Overovanie identity užívateľa vykonáva autentifikovaný subsystém Windows Kerberos dostupný od verzie Windows 2000. Overuje sa identita užívateľa prihláseného do Windows, takže prihlasovanie je automatické bez prihlasovacieho okna a bez zadávania mena a hesla.</p> <p>D2000 Server získa od Windows Kerberos autentifikovaného subsystému informáciu o mene užívateľa a doméne, v ktorej je prihlásený. Pokiaľ názov domény zodpovedá konfigurovanému parametru Doména, poda užívateľského mena vyhľadá objekt typu Užívateľ a skontroluje, či má užívateľ nakonfigurovanú autentifikáciu metódou Kerberos ako povolenú (parameter Metódy autentifikácie) a či nemá za kázané prihlásenie.</p> <p>Poznámka: Sama o sebe je autentifikovaná metóda Kerberos skoro tak nebezpečná, ako nakonfigurovanie parametrov /AN a /AP, ktoré umožní spustenie procesu HI bez zadania mena a hesla, pokiaľ užívateľ odíde od počítača bez zamknutia pracovnej plochy (zadanie štartovacích parametrov je ešte o niečo menej bezpečné, pretože je z nich možné heslo späť vyčítať, pričom autentifikácia Kerberos umožňuje iba okamžité zneužitie, ale nie zistenie hesla). Preto odporúčame:</p> <ul style="list-style-type: none"> • použiť užívateľov, aby pred odchodom od počítača vždy zamkli pracovnú plochu alebo sa odhlásili, • povolenie Kerberos autentifikácie v zabezpečených priestoroch, kde nehrozí zneužitie, • používanie hardvérových kúov na prihlasovanie užívateľov do Windows (USB token, security card a iné), ktoré po vytiahnutí automaticky zamknú pracovnú plochu. <p>Poznámka: Kerberos autentifikácia je použitá iba vo Windows doméne, nie na samostatnom počítači, pretože vyžaduje softvérovú infraštruktúru, ktorá sa inštaluje iba ako súčasť domény Windows.</p>
SPNEGO	<p>Metóda autentifikácie dostupná až vo verziách novších ako D2000 12.00.061. Overovanie identity webového užívateľa (Tenký klient a Smart Web) vykonáva autentifikovaný subsystém Windows Kerberos dostupný od verzie Windows 2000. Overuje sa identita užívateľa prihláseného do Windows, takže prihlasovanie je v prehliadači automatické bez prihlasovacieho okna a bez zadávania mena a hesla.</p> <p>D2000 Server získa od Windows Kerberos autentifikovaného subsystému informáciu o mene užívateľa a doméne, v ktorej je prihlásený. Pokiaľ názov domény zodpovedá konfigurovanému parametru Doména, poda užívateľského mena vyhľadá objekt typu Užívateľ a skontroluje, či má užívateľ nakonfigurovanú autentifikáciu metódou SPNEGO ako povolenú (parameter Metódy autentifikácie) a či nemá za kázané prihlásenie.</p> <p>Poznámka: SPNEGO autentifikácia je použitá iba vo Windows doméne, nie na samostatnom počítači, pretože vyžaduje softvérovú infraštruktúru, ktorá sa inštaluje iba ako súčasť domény Windows.</p>
RFID	<p>Metóda autentifikácie dostupná od D2000 verzie 9.1.30. Užívateľ sa identifikuje zosnímaním RFID karty. Pre funkčnosť RFID autentifikácie musí byť RFID snímač nainštalovaný na klientskom počítači v niektorom zo sériových COM portov, musí bežať proces D2000 HI s parametrami (parameter konzoly), ktoré zabezpečia, aby dokázal snímač obsluhovať. Vi Nastavenia konzoly - RFID parameter.</p> <p>Po zosnímaní RFID karty môžu nastať dva prípady:</p> <ol style="list-style-type: none"> 1. V D2000 HI nie je otvorená žiadna schéma, ktorá implementuje <ENTRY OnRFID> - vtedy HI automaticky prihlási užívateľa s danou RFID kartou. 2. V D2000 HI je otvorená aspoň jedna schéma, ktorá implementuje <ENTRY OnRFID> - vtedy HI neprihlási užívateľa, ale zavolá udalosť OnRFID do všetkých schém, ktoré túto udalosť implementujú a ponechá obsluhu udalosti na aplikovaný skript.

Poznámka 1: Pre iné operané systémy ako Windows je podporovaná iba autentifikácia D2000.

Poznámka 2: Pre iné metódy autentifikácie ako D2000 je potrebná dynamická knižnica d2auth.dll (nachádza sa v adresári [D2000.EXE\bin](#)).

Poznámka 3: Iné metódy autentifikácie ako D2000 sú podporené pre nasledovné procesy a moduly D2000: [D2000 HI](#), [D2000 GrEditor](#), [D2000 CNF](#), [D2000 Management Console](#), [D2000 DDE Server](#), [D2000 System Console](#), [D2000 Tell](#), [D2000 Browser](#), [D2000 ODBC Driver](#).

Konfigurané parametre autentifikácie

Na konfiguráciu metód a parametrov autentifikácie slúžia nasledovné konfigurané parametre autentifikácie:

Názov parametra	Popis
AuthMethod	Prednastavená metóda autentifikácie, ktorú vyžaduje proces D2000 Server od všetkých prihlasujúcich sa užívateľov. Možné hodnoty parametra sú: <ul style="list-style-type: none">D2000NTLMKerberosSPNEGO (iba pre Tenký klient a SmartWeb)
AuthSecPrinc	Security principal autentifikácie. Parameter je vyžadovaný v Kerberos a SPNEGO autentifikácii. Security principal môže byť názov útu, pod ktorým je spustený proces D2000 Server . Štandardne (kernel.exe je spustený ako servis pod útom <i>Local System</i>) je <i>Security principal</i> účet počítača v doméne, ktorého názov je rovnaký ako názov počítača a na konci má znak dolár (\$). Pokiaľ je proces kernel.exe spustený ručne (z príkazového riadku), je <i>Security principal</i> účet príslušného užívateľa v doméne. Príklad: Doména je MyCompany, server je SrvApp1, proces kernel.exe je spustený ako servis pod útom <i>Local System</i> . Parameter AuthSecPrinc môže byť <i>srvapp1\$</i> alebo <i>srvapp1\$@MyCompany</i> . Pokiaľ sa chcú autentifikovať aj užívatelia z inej domény OtherCompany, musí byť AuthSecPrinc= <i>srvapp1\$@MyCompany</i> a navyše doména MyCompany musí dôverovať doméne OtherCompany. Poznámka: autentifikácia medzi doménami bola vyskúšaná na serveri srvapp114v v doméne ipstest.sk, AuthSecPrinc= <i>srvapp114v\$@ipstest.sk</i> . HI bolo spustené na počítači v doméne IPESoft, doména ipstest.sk dôverovala doméne IPESoft. Príklad: Doména je MyCompany, proces kernel.exe je spustený z príkazového riadka užívateľom D2User. Parameter AuthSecPrinc môže byť <i>d2user</i> alebo <i>d2user@MyCompany</i> . Poznámka: Pomocou nástrojov na správu Active Directory je možné definovať aj Security principal, ktorý nie je závislý od mena užívateľa, pod ktorým je proces kernel.exe spustený. Viac informácií viď dokumentácia k Active Directory a k utilite ktpass.exe na webe Microsoftu.

Paralelné použitie viacerých autentifikovaných metód

Pri autentifikácii NTLM/Kerberos sa užívateľské meno ani heslo neprenáša medzi počítačom s procesom [D2000 Server](#) a počítačom, kde beží užívateľský proces (HI, CNF, GrEditor at.). Miesto toho sa po sieti prenášajú iba tzv. tokeny, ktoré si vymieňajú autentifikované subsystemy Windows NTLM/Kerberos medzi týmito počítačmi a radiom domény. Preto autentifikácia NTLM/Kerberos nebude fungovať, pokiaľ je doménový radi (domain controller) nedostupný (porucha / vypnutie doménového radia, prístup klienta spoza firewallu at.).

Z týchto dôvodov, ako aj z dôvodov konfiguranej flexibility, môže klientsky proces (HI, CNF, GrEditor at.) použiť inú metódu autentifikácie, ako je štandardná nakonfigurovaná parametrom [AuthMethod](#) za predpokladu, že:

- pre zvolenú metódu sú správne nakonfigurované všetky [konfigurané parametre](#) (t.j. [Doména](#) pre NTLM/Kerberos a [AuthSecPrinc](#) pre Kerberos),
- užívateľ má povolenú zvolenú autentifikovanú metódu vo svojich [Metódach autentifikácie](#).

Výber inej metódy autentifikácie je možný pomocou štartovacieho parametra klientskeho procesu [/AF<Method>](#), v prípade [D2000 ODBC Driver](#) sa metóda autentifikácie explicitne konfiguruje v [konfigurácii DSN](#).

Poznámka: Proces D2000 Server pri každom prihlásení sa procesu, ktorý podporuje prihlasovanie užívateľa (HI, CNF, GrEditor at.), naíť konfigurované parametre autentifikácie z Windows registry a pošle ich prihlasujúcemu sa procesu. Je to kvôli možnosti dynamicky zmeniť prednastavenú metódu autentifikácie počas behu systému D2000 (napr. počas výpadku doménového radia) a umožniť tak užívateľom, aby reštartovali HI a prihlásili sa do aplikácie inou autentifikovanou metódou ([D2000](#)) bez potreby upravovania štartovacích parametrov HI konzol všetkých užívateľov. Samozrejme takýto scenár vyžaduje, aby každý užívateľ mal povolenú autentifikovanú metódu [D2000](#) a navyše poznal svoje "záložné" heslo do D2000 uložené v konfigurácii užívateľa.

Debugovanie autentifikácie

Na debugovanie autentifikácie slúži kategória Debug informácií **DBG.Authentication**, ktorá sa dá zapnúť pri štarte procesu štartovacím parametrom [/E+DBG.Authentication](#) alebo počas behu procesu pomocou [D2000 System Console](#).

Po zapnutí debugovania bude log procesu [D2000 Server](#) alebo log klientskeho procesu (HI, CNF, GrEditor at.) obsahovať podrobné výpisy o jednotlivých fázach autentifikácie (pre [NTLM](#) a [Kerberos](#) autentifikáciu), ktoré sú použité na účely technickej podpory.



Súvisiace stránky:

[Konfigurácia aplikácie](#)