

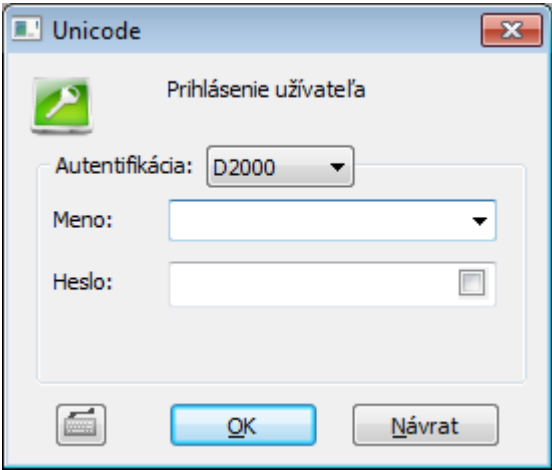
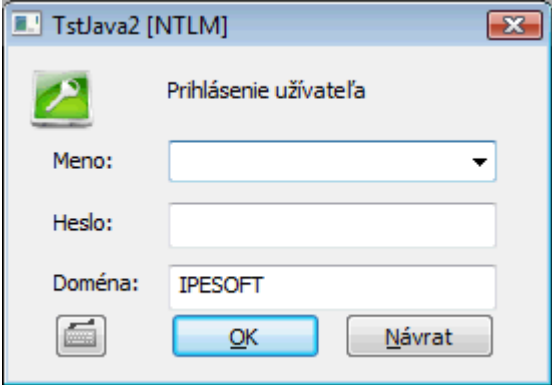
# Autentifikácia v D2000

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 (prihlasovacie meno + heslo), o vlastní (prihlasovací USB token, osobná IPová karta so šifrovaním a identifikovaným 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](#)),
- zabezpečiť prihlásenie užívateľa do D2000 hardvérovou (prihlasovací USB token, osobná IPová karta so šifrovaním a identifikovaným 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 mať heslo do D2000, nástrojmi pre správu užívateľov v doméne Windows.

## Metódy autentifikácie

V systéme D2000 sú od verzie 7.02.008 podporované nasledovné metódy autentifikácie:

Metóda autentifikácie	Popis
D2000	<p>Overovanie užívateľského mena a hesla procesom <a href="#">D2000 Server</a>. Toto je štandardná metóda autentifikácie, ktorá využíva meno a heslo uložené v konfigurácii objektu <a href="#">Užívateľ</a>. Prihlasovací dialóg zobrazuje užívateľské meno a heslo:</p> 
NTLM	<p>Overovanie mena a hesla zadávaného 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 <a href="#">Doména</a>. <a href="#">D2000 Server</a> získa po dokončení autentifikácie od Windows informáciu o úspešnom/neúspešnom overení užívateľského mena a hesla v doméne. Pokiaľ bola autentifikácia úspešná, podľa užívateľského mena vyhľadá objekt typu <a href="#">Užívateľ</a> a skontroluje, či má užívateľ nakonfigurovanú autentifikáciu metódou NTLM ako povolenú (parameter <a href="#">Metódy autentifikácie</a>), či je zhodný názov domény a či nemá <a href="#">zakázané prihlásenie</a>. 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><b>Poznámka:</b> NTLM autentifikácia je použitá na samostatnom počítači s lokálne definovanými užívateľmi (vtedy <a href="#">Doména</a> je názov počítača) ako aj vo Windows doméne (<a href="#">Doména</a> je názov domény). Ak nie je možné kontaktovať autentifikáciu autoritu, prihlásenie neprebehne. Prihlasovanie sa zmení na autentifikáciu podľa <a href="#">D2000</a> a užívateľovi sa zobrazí upozornenie "Neúspešná NTLM autentifikácia. Zadajte 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. <a href="#">D2000 Server</a> získa od Windows Kerberos autentifikovaného subsystému informáciu o mene užívateľa a doméne, v ktorej je prihlásený. Pokiaľ názov domény zodpovedá konfiguračnému parametru <b>Doména</b>, podľa užívateľského mena vyhľadá objekt typu <b>Užívateľ</b> a skontroluje, či má užívateľ nakonfigurovanú autentifikáciu metódou Kerberos ako povolenú (parameter <b>Metódy autentifikácie</b>) a či nemá <b>zakázané prihlásenie</b>.</p> <p><b>Poznámka:</b> Sama o sebe je autentifikovaná metóda Kerberos skoro tak nebezpečná, ako nakonfigurovanie parametrov <b>/AN</b> a <b>/AP</b>, ktoré umožnia 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 získanie hesla). Preto odporúčame:</p> <ul style="list-style-type: none"> <li>použitie užívateľov, aby pred odchodom od počítača vždy zamkli pracovnú plochu alebo sa odhlásili,</li> <li>povolenie Kerberos autentifikácie v zabezpečených priestoroch, kde nehrozí zneužitie,</li> <li>používanie hardvérových kúrov na prihlasovanie užívateľov do Windows (USB token, security card a iné), ktoré po vytiahnutí automaticky zamknú pracovnú plochu.</li> </ul> <p><b>Poznámka:</b> Kerberos autentifikácia je použitá iba vo Windows doméne, nie na samostatnom počítači, pretože vyžaduje softvérovú infraštruktúru, ktorá sa inštaluje iba ako súčasť radia domény Windows.</p>
TCL	<p>Metóda autentifikácie dostupná až od D2000 verzie 8.00.002, ktorú môžu využívať iba užívatelia typu <b>Tenký klient</b> používajúci internetové prehliadače s podporou Kerberos autentifikácie (napr. Internet Explorer, Mozilla Firefox, Google Chrome), nachádzajúci sa na firemnom intranete a prihlásení do domény <b>Doména</b>. TCL autentifikácia vyžaduje <b>inštaláciu</b> autentifikovaného rozšírenia <b>tomcatssnego</b> do Apache Tomcat webservera.</p> <p>Overovanie identity užívateľa prebieha medzi internetovým prehliadačom a korektným nastaveným <b>web serverom</b> za použitia autentifikovaného subsystému Windows Kerberos. Overuje sa identita užívateľa prihláseného do Windows, takže prihlasovanie je automatické bez prihlasovacieho okna a bez zadávania mena a hesla.</p> <p>Po úspešnom overení sú procesu <b>D2000 Server</b> poslané informácie o mene užívateľa a doméne, v ktorej je prihlásený. Pokiaľ názov domény zodpovedá konfiguračnému parametru <b>Doména</b>, podľa užívateľského mena vyhľadá objekt typu <b>Užívateľ</b> a skontroluje, či má užívateľ nakonfigurovanú autentifikáciu metódou TCL ako povolenú (parameter <b>Metódy autentifikácie</b>) a či nemá <b>zakázané prihlásenie</b>.</p> <p><b>Poznámka:</b> Pokiaľ užívateľ nie je vo Windows doméne alebo neprebehne úspešne Kerberos autentifikácia, zobrazí sa prihlasovacie okno vyzývajúce na zadanie mena a hesla. Tieto sa používajú pri následnom prihlasovaní za použitia <b>D2000</b> autentifikácie.</p>
RFID	<p>Metóda autentifikácie dostupná od D2000 verzie 9.1.30. Užívateľ sa identifikuje zosnímaním RFID karty. Pre funkciu RFID autentifikácie musí byť RFID snímač nainštalovaný na klientskom počítači v niektorom zo sériových COM portov, musí bežať proces D2000 HI s parametrami (parametre konzoly), ktoré zabezpečia, aby dokázal snímač obsluhovať. Vi <b>Nastavenia konzoly</b> - RFID parametre.</p> <p>Po zosnímaní RFID karty môžu nastať dva prípady:</p> <ol style="list-style-type: none"> <li>V D2000 HI nie je otvorená žiadna schéma, ktorá implementuje &lt;ENTRY OnRFID&gt; - vtedy HI automaticky prihlási užívateľa s danou RFID kartou.</li> <li>V D2000 HI je otvorená aspoň jedna schéma, ktorá implementuje &lt;ENTRY OnRFID&gt; - vtedy HI neprihlási užívateľa, ale zavolá udalosť <b>OnRFID</b> do všetkých schém, ktoré túto udalosť implementujú a ponechá obsluhu udalosti na aplikovaný skript.</li> </ol>

**Poznámka 1:** Pre iné operované 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**.

## Konfiguračné parametre autentifikácie

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

Názov parametra	Popis
AuthMethod	<p>Prednastavená metóda autentifikácie, ktorú vyžaduje proces <b>D2000 Server</b> od všetkých prihlasujúcich sa užívateľov. Možné hodnoty parametra sú:</p> <ul style="list-style-type: none"> <li><b>D2000</b></li> <li><b>NTLM</b></li> <li><b>Kerberos</b></li> </ul> <p><b>Poznámka:</b> Metóda <b>TCL</b> nemôže byť nastavená ako hodnota tohto parametra - táto metóda je implicitne povolená pre užívateľov typu <b>Tenký klient</b> a zakázaná pre všetky ostatné procesy.</p>
AuthSecPrinc	<p>Security principal autentifikácie. Parameter je vyžadovaný v <b>Kerberos</b> autentifikácii.</p> <p>Security principal môže byť názov útu, pod ktorým je spustený proces <b>D2000 Server</b>. Štandardne (kernel.exe je spustený ako servis pod útom <b>Local System</b>) je <b>Security principal</b> útom 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 <b>Security principal</b> útom príslušného užívateľa v doméne.</p> <p><b>Príklad:</b> Doména je MyCompany, server je SrvApp1, proces kernel.exe je spustený ako servis pod útom <b>Local System</b>. Parameter AuthSecPrinc môže byť <b>srvapp1\$</b> alebo <b>srvapp1\$@MyCompany</b>. Pokiaľ sa chcú autentifikovať aj užívatelia z inej domény OtherCompany, musí byť AuthSecPrinc=<b>srvapp1\$@MyCompany</b> a navyše doména MyCompany musí dôverovať doméne OtherCompany.</p> <p><b>Poznámka:</b> autentifikácia medzi doménami bola vyskúšaná na serveri srvapp114v v doméne ipstest.sk, AuthSecPrinc=<b>srvapp114v\$@ipstest.sk</b> HI bolo spustené na počítači v doméne IPESoft, doména ipstest.sk dôverovala doméne IPESoft.</p> <p><b>Príklad:</b> Doména je MyCompany, proces kernel.exe je spustený z príkazového riadka užívateľom D2User. Parameter AuthSecPrinc môže byť <b>d2user</b> alebo <b>d2user@MyCompany</b>.</p> <p><b>Poznámka:</b> 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 vi dokumentácia k Active Directory a k utilite <b>ktpass.exe</b> na webe Microsoftu.</p>

## 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 subsystémy Windows NTLM/Kerberos medzi týmito počítačmi a radiom domény. Preto autentifikácia NTLM/Kerberos nebude fungovať, pokiaľ je doménový riadič (domain controller) nedostupný (porucha /vypnutie doménového radia, prístup klienta spoza firewallu at.).

Z týchto dôvodov, ako aj z dôvodov konfiguračnej 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 autentifikáciu 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), načíta konfigurané 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 umožní 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 autentifikáciu 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 pre účely technickej podpory.



### Súvisiace stránky:

[Konfigurácia aplikácie](#)