



Richard Komžík

20070515

Trojhlavý pes a iní démoni

IT bezpečnosť na AsÚ SAV

NETnews



Trojhlavý pes a iní démoni

DÔVODY, CIELE

- konsolidácia
- rastúci počet užívateľov, počítačov
- príliš veľa kônt, hesiel - **Kerberos**
- príliš veľa rozdrobeného diskového priestoru - **LDAP**
- zjednodušenie administrácie účtov
- bezpečnosť



Trojhlavý pes a iní démoni

ZÁKLADNÉ POJMY

- **AAA**
- **autentifikácia - Authentication** - preukázanie, že som ten, za koho sa vyhlasujem
 - čo som - odtlačok prsta, dúhovka, DNA - xerox odtlačku
 - čo mám - HW kľúč - odcudzenie
 - čo viem - heslo - kompromitácia, slovníkový útok
- **autorizácia - Authorization** - preukázanie, že mám oprávnenie vykonávať nejakú činnosť, používať určitú službu
- **účty - Accounting**



Trojhlavý pes a iní démoni

- **šifrovanie**
 - **symetrické**
 - jeden kľúč pre zašifrovanie aj rozšifrovanie
 - problém prenosu kľúča v nedôveryhodnom prostredí
 - **asymetrické**
 - verejný a tajný kľúč
 - fungujú iba v páre: šifruje sa verejným, dešifruje tajným a vice versa
 - hashovacia suma: charakterizuje vstup, jednocestnosť
 - problémy:
 - výpočtovo náročnejšie
 - dôveryhodnosť verejného kľúča – certifikačná autorita
 - kompromitácia MD5, SHA1
 - využitie: šifrovanie, elektronické podpisovanie



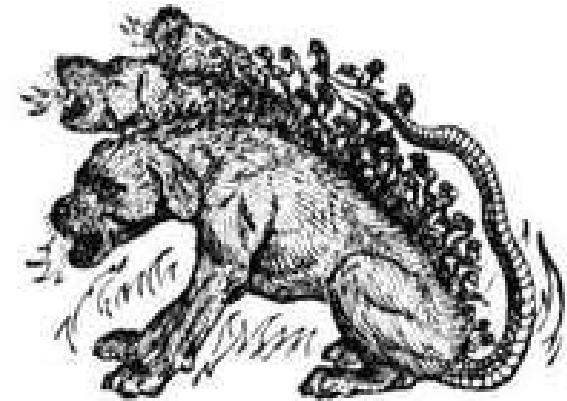
Trojhlavý pes a iní démoni

<http://en.wikipedia.org/wiki/Cerberus>



Κέρβερος

Kerberos



Cerberus



Trojhlavý pes a iní démoni

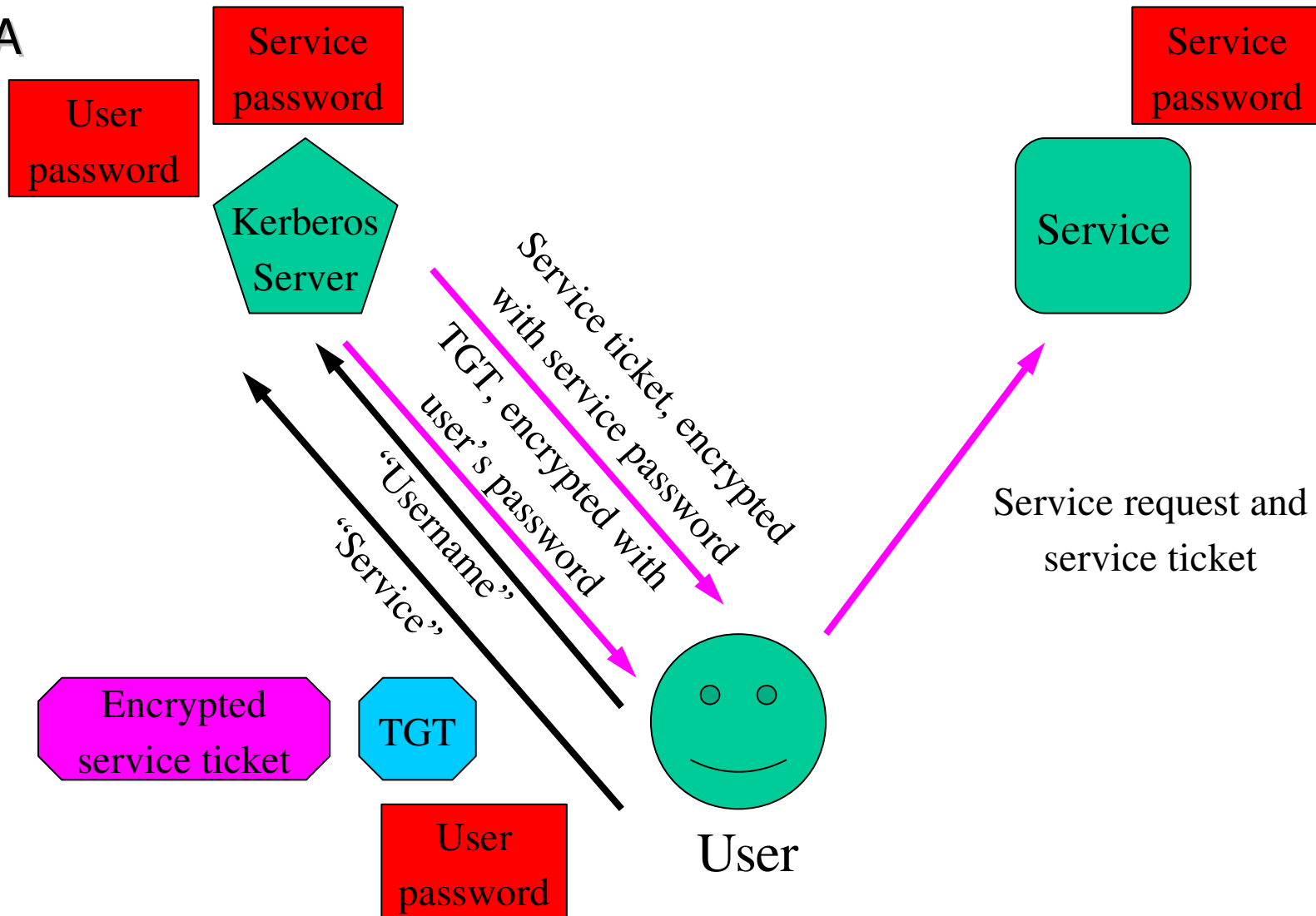
KERBEROS

- autentifikačný protokol (staršie spôsoby NIS/Yellow Pages, NIS+)
- viacero verzií: Heimdal, MIT v.5
- ukladá, spravuje login/password
- symetrické šifrovanie
- dôveryhodná tretia strana/inštancia
- principals pre užívateľov, služby
- vydáva časovo obmedzené lístky: tickets/credentials
- cieľ: 'single-sign-on' system



Trojhlavý pes a iní démoni

SCHÉMA





Trojhlavý pes a iní démoni

PROBLÉMY/UPOZORNENIA

- nie všetky služby podporujú Kerberos
- potreba dobrej synchronizácie času - NTP
- závislosť na kerberos-servri, ideálne: replikovaný, dedikovaný
- prihlásiť sa môže len ten, kto má platný lokálny účet
- nepoužívať kerberos pre root-a

VÝHODY

- jedno prihlásenie na 8 hodín: ssh, scp, www/w3, ftp, telnet
- heslá nie sú po sieti vôbec prenášané



Trojhlavý pes a iní démoni

POUŽITIE

- zadať na kerberos-servri principal pre užívateľa a jeho počítač
- nakonfigurovať počítač užívateľa
 - REALM: TA3.SK
 - kerberos server: auriga.ta3.sk = kerberos.ta3.sk, kerberos2.ta3.sk
 - DNS
- kinit; klist; kpasswd; kdestroy



Trojhlavý pes a iní démoni

WINDOWS

- nainštalovať ksetup.exe z \support\tools\support.cab - teda inštalačné CD: \support\tools\setup - zaškrtnúť *complete*
 - *ksetup /setrealm TA3.SK*
 - *ksetup /addkdc TA3.SK kerberos.ta3.sk*
 - *ksetup /addkdc TA3.SK kerberos2.ta3.sk*
 - *ksetup /mapuser * **
- konfigurácia kerberos je uložená v
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos
- M\$ si vybral Kerberos ako autentifikačný protokol



Trojhlavý pes a iní démoni

LINUX

- `/etc/krb5.conf`
- `/etc/pam.d/system-auth`
- `authconfig --enablekrb5 --krb5kdc=kerberos.ta3.sk \
--krb5adminserver=kerberos.ta3.sk --krb5realm=TA3.SK \
--enablekrb5kdcdns --enablekrb5realmdns --update`
- klíč: `/etc/krb5.keytab`
- ssh, scp
 - `/etc/ssh/sshd_config`
 - `KerberosAuthentication yes`
 - `KerberosOrLocalPasswd yes`
 - `GSSAPIAuthentication yes`
 - `/etc/ssh/ssh_config`
 - `GSSAPIAuthentication yes`



Trojhlavý pes a iní démoni

LDAP

- Lightweight Directory Access Protocol, X500
- adresárová služba – menšie súbory, prevažne čítanie
- do adresára sa dajú uložiť rôzne potrebné informácie
- autorizácia – kto smie využívať aké služby
- cieľ: vytvoriť jednotný priestor (diskový priestor, najrôznejšie informácie) pre všetkých užívateľov, nezávisle na ich OS
- výhody: centralizovaná správa, zálohovanie



Trojhlavý pes a iní démoni

DROBNOSTI

- programovanie v shelli
 - *for i in `ls *.FITS`; do k=`echo \$i | tr A-Z a-z` ; echo \$i \$k;
convert -geometry 30% \$i \$k ; done*
 - wildcards = žolíkové znaky, regulárne výrazy:
*ls -l [c-o,x]*1?.fits*
- grafické knižnice pre FORTRAN
 - pgplot <http://www.astro.caltech.edu/~tjp/pgplot/>
 - pilib <http://sourceforge.net/projects/pilib/>
 - dislin <http://www.dislin.de>



Trojhlavý pes a iní démoni

OTÁZKY

- greylisting - antiSPAM nástroj
 - zdržiava, väčšia záťaž pre server

INCIATÍVY

- SANET – pre diakritiku používať UTF-8

VoIP

- natívne IP telefóny v Bratislave, Lomnickom štíte
- Úrad SAV na VoIP/SIP
 - http://www.urad.sav.sk/files/phone_zoznam_new.htm
 - 02/57510???
 - http://auriga.ta3.sk/VoIP/check_enum.php



Trojhlavý pes a iní démoni

HARDWARE

- Komisia P SAV pre informačné a komunikačné technológie
- účelovo pridelované prostriedky areálom
- posledné 3 roky po 200 000.-Sk
- VoIP
- obnova servrov, rack chassis
- gemini – NTP server
- indus – log server
- auriga (80 000.-Sk na konci roku 2006)
- racky
- klimatizácia



Trojhlavý pes a iní démoni

HARDWARE - BEŽNÉ

- IP telefóny Bratislava
- sieťová laserová tlačiareň na spodnú chodbu
- HUBy vs. switche
- 11 Mbps rádio na Lomnický štít
- optika na Lomnickom štíte



Trojhlavý pes a iní démoni

HARDWARE - POTREBNÉ

- natívne IP telefóny – paušál ST
- cygnus – WWW



Mercury



USB



WYKONANIE PRAC
MONTAŻ
SERWIS
CZYSZCZENIE

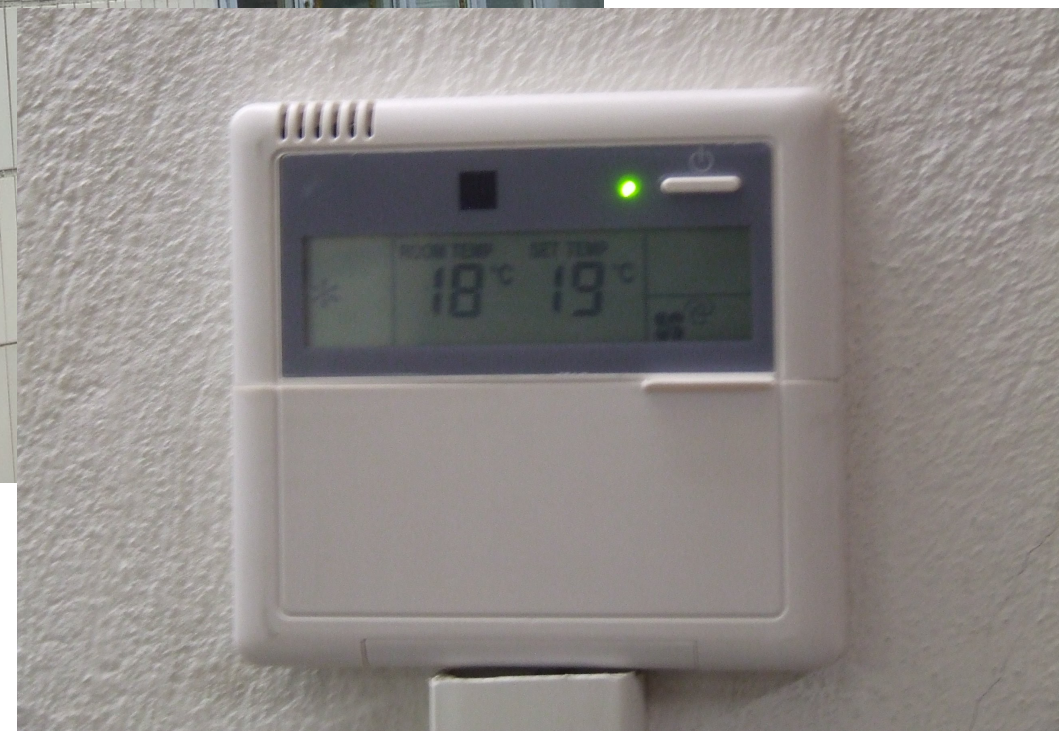
ASUS

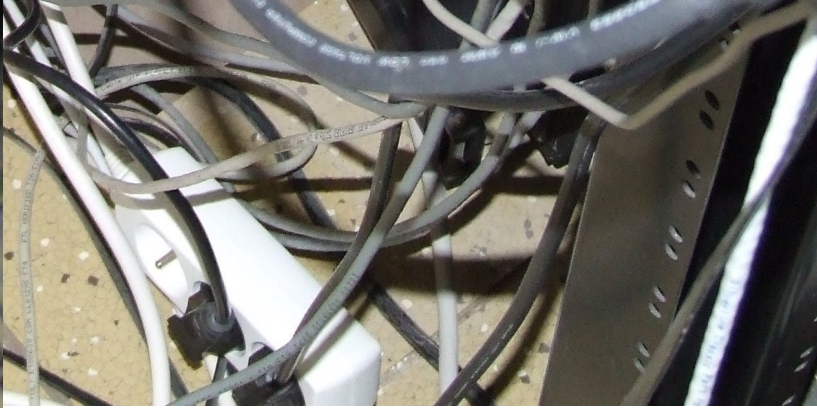
zakopane.pl, www.zakopane.pl
Orbis Travel
LICY
NICZE
OKAROWE
IMOWE
RYSTYKA
JOWA, ZAGRANICZNA
pane
ppówki 22
Nowy Targ
ul. Kolejowa 21
tel. (18) 28 666
pane.pl
cyf Podhal
kasy fiskalne
serwis • usługi
Internet R













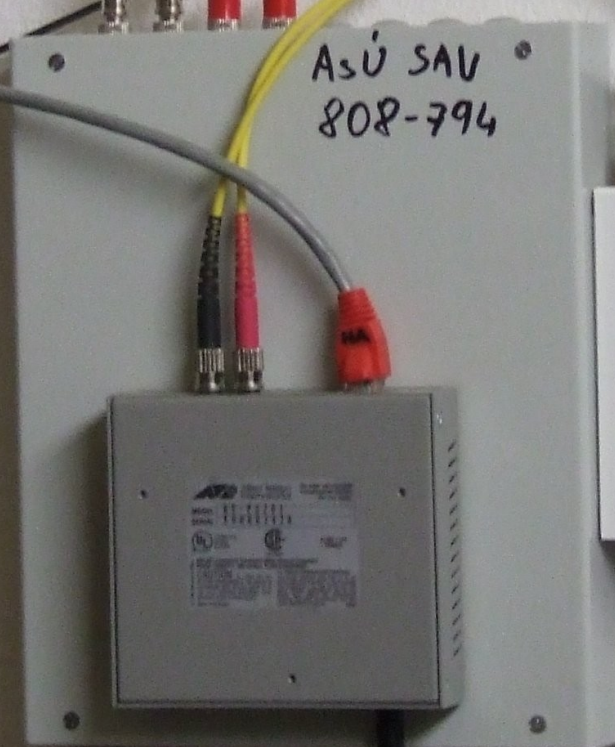
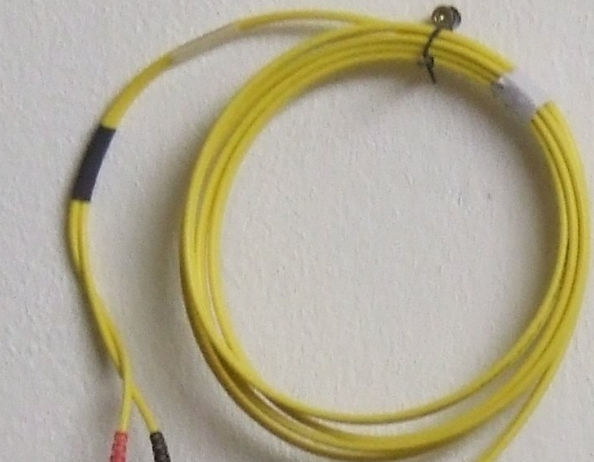


| Account | Balance | Debit | Credit | Balance |
|----------|----------|-------|--------|----------|
| 001-1000 | 100.00 | | | 100.00 |
| 001-1001 | 200.00 | | | 200.00 |
| 001-1002 | 300.00 | | | 300.00 |
| 001-1003 | 400.00 | | | 400.00 |
| 001-1004 | 500.00 | | | 500.00 |
| 001-1005 | 600.00 | | | 600.00 |
| 001-1006 | 700.00 | | | 700.00 |
| 001-1007 | 800.00 | | | 800.00 |
| 001-1008 | 900.00 | | | 900.00 |
| 001-1009 | 1000.00 | | | 1000.00 |
| 001-1010 | 1100.00 | | | 1100.00 |
| 001-1011 | 1200.00 | | | 1200.00 |
| 001-1012 | 1300.00 | | | 1300.00 |
| 001-1013 | 1400.00 | | | 1400.00 |
| 001-1014 | 1500.00 | | | 1500.00 |
| 001-1015 | 1600.00 | | | 1600.00 |
| 001-1016 | 1700.00 | | | 1700.00 |
| 001-1017 | 1800.00 | | | 1800.00 |
| 001-1018 | 1900.00 | | | 1900.00 |
| 001-1019 | 2000.00 | | | 2000.00 |
| 001-1020 | 2100.00 | | | 2100.00 |
| 001-1021 | 2200.00 | | | 2200.00 |
| 001-1022 | 2300.00 | | | 2300.00 |
| 001-1023 | 2400.00 | | | 2400.00 |
| 001-1024 | 2500.00 | | | 2500.00 |
| 001-1025 | 2600.00 | | | 2600.00 |
| 001-1026 | 2700.00 | | | 2700.00 |
| 001-1027 | 2800.00 | | | 2800.00 |
| 001-1028 | 2900.00 | | | 2900.00 |
| 001-1029 | 3000.00 | | | 3000.00 |
| 001-1030 | 3100.00 | | | 3100.00 |
| 001-1031 | 3200.00 | | | 3200.00 |
| 001-1032 | 3300.00 | | | 3300.00 |
| 001-1033 | 3400.00 | | | 3400.00 |
| 001-1034 | 3500.00 | | | 3500.00 |
| 001-1035 | 3600.00 | | | 3600.00 |
| 001-1036 | 3700.00 | | | 3700.00 |
| 001-1037 | 3800.00 | | | 3800.00 |
| 001-1038 | 3900.00 | | | 3900.00 |
| 001-1039 | 4000.00 | | | 4000.00 |
| 001-1040 | 4100.00 | | | 4100.00 |
| 001-1041 | 4200.00 | | | 4200.00 |
| 001-1042 | 4300.00 | | | 4300.00 |
| 001-1043 | 4400.00 | | | 4400.00 |
| 001-1044 | 4500.00 | | | 4500.00 |
| 001-1045 | 4600.00 | | | 4600.00 |
| 001-1046 | 4700.00 | | | 4700.00 |
| 001-1047 | 4800.00 | | | 4800.00 |
| 001-1048 | 4900.00 | | | 4900.00 |
| 001-1049 | 5000.00 | | | 5000.00 |
| 001-1050 | 5100.00 | | | 5100.00 |
| 001-1051 | 5200.00 | | | 5200.00 |
| 001-1052 | 5300.00 | | | 5300.00 |
| 001-1053 | 5400.00 | | | 5400.00 |
| 001-1054 | 5500.00 | | | 5500.00 |
| 001-1055 | 5600.00 | | | 5600.00 |
| 001-1056 | 5700.00 | | | 5700.00 |
| 001-1057 | 5800.00 | | | 5800.00 |
| 001-1058 | 5900.00 | | | 5900.00 |
| 001-1059 | 6000.00 | | | 6000.00 |
| 001-1060 | 6100.00 | | | 6100.00 |
| 001-1061 | 6200.00 | | | 6200.00 |
| 001-1062 | 6300.00 | | | 6300.00 |
| 001-1063 | 6400.00 | | | 6400.00 |
| 001-1064 | 6500.00 | | | 6500.00 |
| 001-1065 | 6600.00 | | | 6600.00 |
| 001-1066 | 6700.00 | | | 6700.00 |
| 001-1067 | 6800.00 | | | 6800.00 |
| 001-1068 | 6900.00 | | | 6900.00 |
| 001-1069 | 7000.00 | | | 7000.00 |
| 001-1070 | 7100.00 | | | 7100.00 |
| 001-1071 | 7200.00 | | | 7200.00 |
| 001-1072 | 7300.00 | | | 7300.00 |
| 001-1073 | 7400.00 | | | 7400.00 |
| 001-1074 | 7500.00 | | | 7500.00 |
| 001-1075 | 7600.00 | | | 7600.00 |
| 001-1076 | 7700.00 | | | 7700.00 |
| 001-1077 | 7800.00 | | | 7800.00 |
| 001-1078 | 7900.00 | | | 7900.00 |
| 001-1079 | 8000.00 | | | 8000.00 |
| 001-1080 | 8100.00 | | | 8100.00 |
| 001-1081 | 8200.00 | | | 8200.00 |
| 001-1082 | 8300.00 | | | 8300.00 |
| 001-1083 | 8400.00 | | | 8400.00 |
| 001-1084 | 8500.00 | | | 8500.00 |
| 001-1085 | 8600.00 | | | 8600.00 |
| 001-1086 | 8700.00 | | | 8700.00 |
| 001-1087 | 8800.00 | | | 8800.00 |
| 001-1088 | 8900.00 | | | 8900.00 |
| 001-1089 | 9000.00 | | | 9000.00 |
| 001-1090 | 9100.00 | | | 9100.00 |
| 001-1091 | 9200.00 | | | 9200.00 |
| 001-1092 | 9300.00 | | | 9300.00 |
| 001-1093 | 9400.00 | | | 9400.00 |
| 001-1094 | 9500.00 | | | 9500.00 |
| 001-1095 | 9600.00 | | | 9600.00 |
| 001-1096 | 9700.00 | | | 9700.00 |
| 001-1097 | 9800.00 | | | 9800.00 |
| 001-1098 | 9900.00 | | | 9900.00 |
| 001-1099 | 10000.00 | | | 10000.00 |

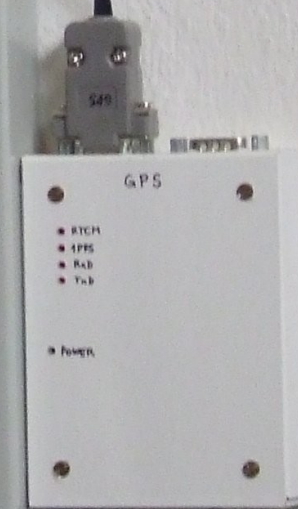
Wednesday March 28, 2007







ASÚ SAV
808-794



GPS

- RTCM
- SPFS
- RAB
- TWB

- POWER







Trojhlavý pes a iní démoni

ĎAKUJEM ZA POZORNOST