Návod na odblokování tokenu eToken 5110 CC

Obsah

1) Jak poznat pro kterou certifikační autoritu je token určen? 2
2) Token jsem pořídil/a od certifikační autority PostSignum 4
   a) V případě zablokování Hesla k tokenu – počet 0 7
   b) V případě zablokování Digital Signature PIN –počet 0 9
   c) V případě zablokování Digital Signature PUK –počet 0 11
3) Token jsem pořídil/a od certifikační autority eIdentity 12
   a) V případě zablokování Hesla k tokenu – počet 0 14
   b) V případě zablokování Digital Signature PIN – počet 0 16
   c) V případě zablokování Digital Signature PUK – počet 0 18

1) Jak poznat pro kterou certifikační autoritu je token určen?

Nejjednodušší cestou ke zjištění je zeptat se dodavatele tokenu.

Aktuálně do kvalifikovaných prostředků eToken 5110 CC vydávají kvalifikované certifikáty dvě certifikační autority.

Certifikační autorita PostSignum Česká pošta

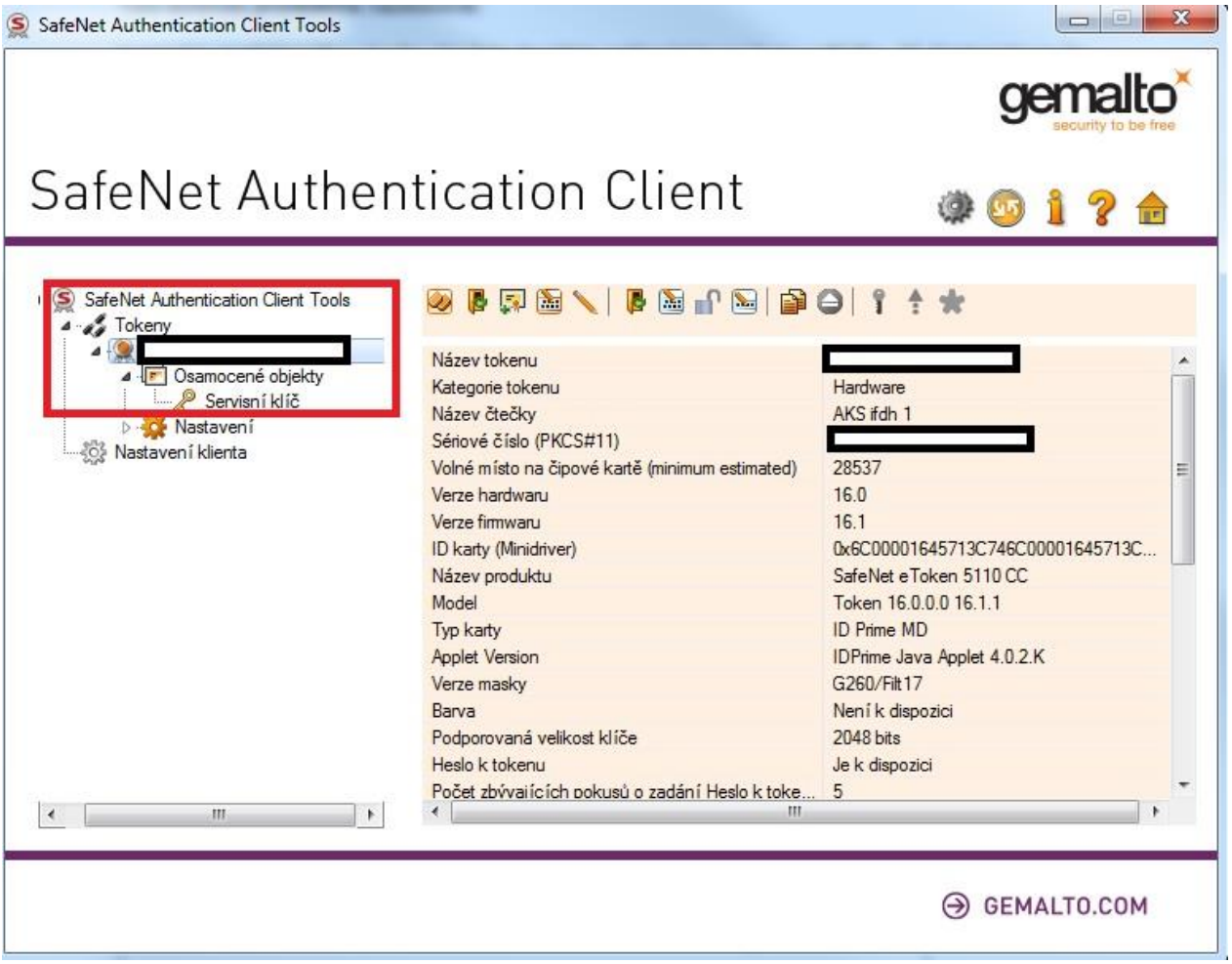
Certifikační autorita eIdentity

Certifikační autorita **PostSignum** do tokenů přednahrává speciální klíč, který zajistí bezpečnou identifikaci předmětu v programu iSignum (používá se pro zažádání o obnovu a generování nového kvalifikovaného certifikátu).

Certifikační autorita eIdentity provádí generování certifikátu přímo do tokenu.

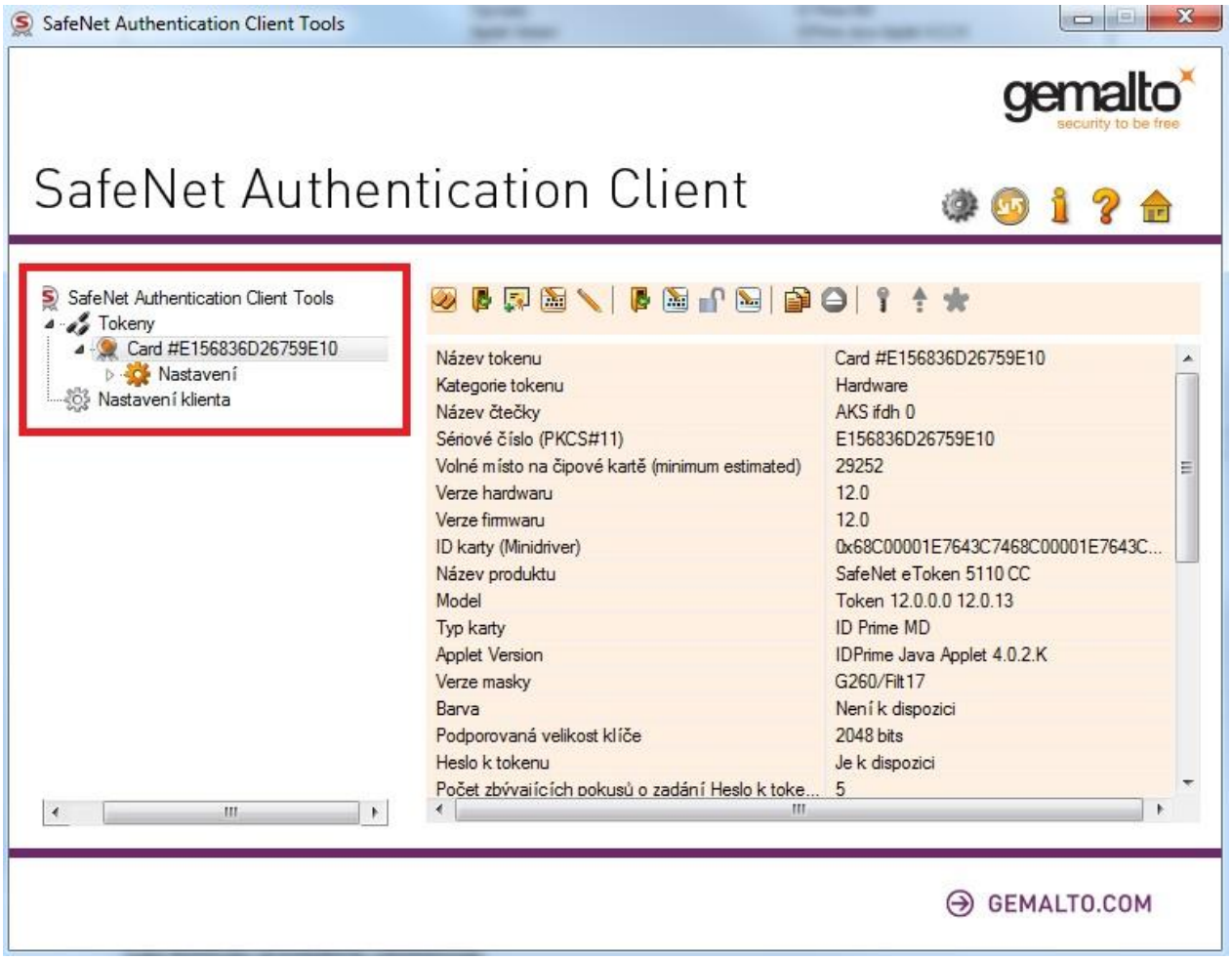
Pokud Váš autentizační předmět obsahuje „**Servisní klíč**“, s největší pravděpodobností máte, nebo budete chtít využívat certifikátů PostSignum.

Token se Servisním Klíčem:



V případě, že token neobsahuje žádnou položku „Servisní klíč“, bude se jednat o token určený pro certifikační autoritu PostSignum.

Token bez Servisního klíče:



Do tohoto podrobného zobrazení se dostanete po kliknutí na „ozubené kolo“ v horní části okna.

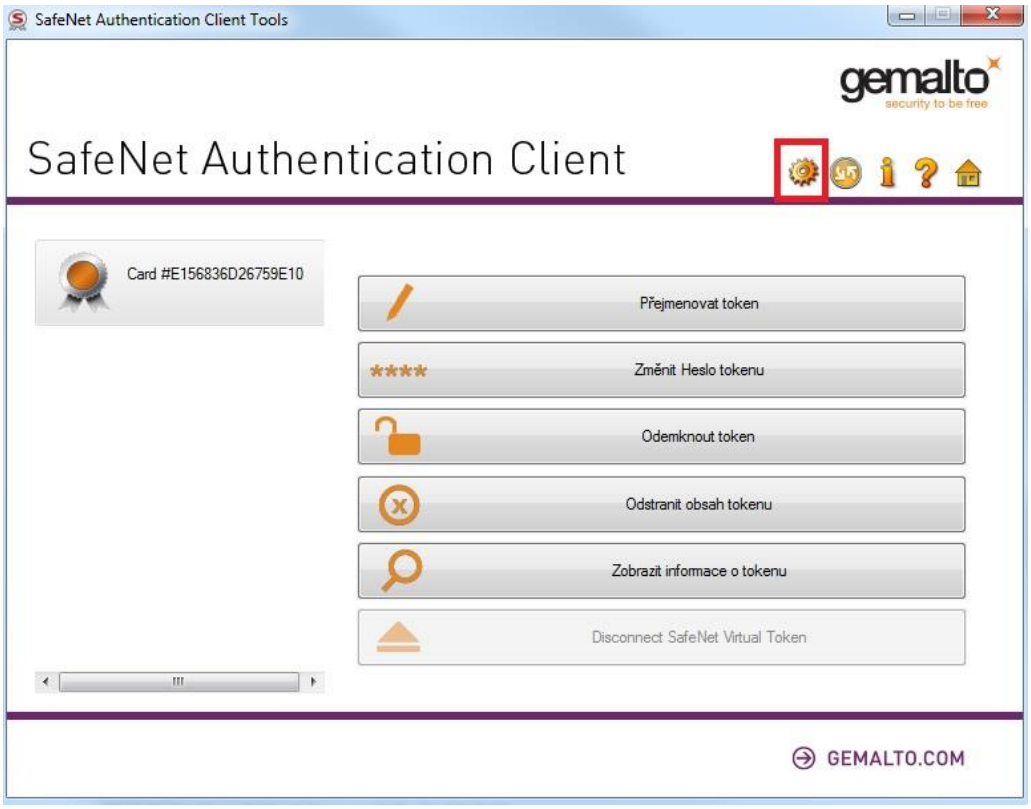
2) Token jsem pořídil/a od certifikační autority PostSignum

V případě zakoupení kvalifikovaného prostředku pro vytváření kvalifikovaného podpisu eToken 5110 CC od certifikační autority PostSignum prosím nejdříve zkontrolujte přítomnost „Osamoceného objektu“ s názvem Servisní klíč.

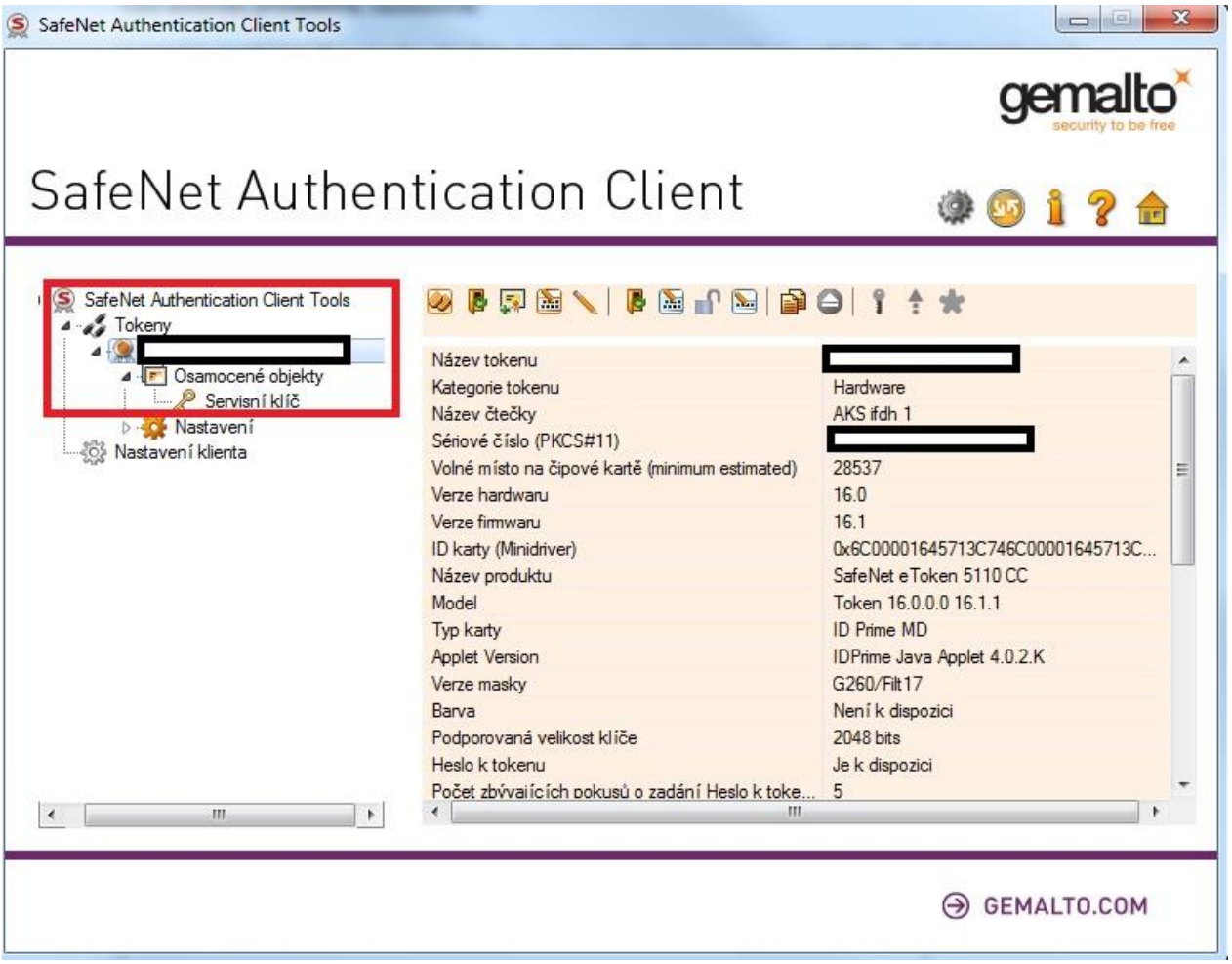
Tuto kontrolu provedeme následovně:

V pravém spodním rohu u hodin otevřete dvojitým poklepáním na ikonu svítícího „S“. Dostanete se do „Jednoduchého zobrazení“ kde vidíme možnosti jako: Přejmenovat token, Změnit heslo k tokenu, Odemknout token, atd.

Nyní zvolíme možnost rozšířeného zobrazení pomocí ikony ozubeného kola ve vrchní části obrazovky.



V rozšířeném zobrazení zkontrolujeme levý sloupec, kde vidíme náš připojený token. Rozkliknutím tohoto tokenu se zobrazí obsah tokenu, kde je vidět kvalifikovaný certifikát (CC certifikáty). Současně by měl být vidět kontejner „Osamocené objekty“ a v něm Servisní klíč.



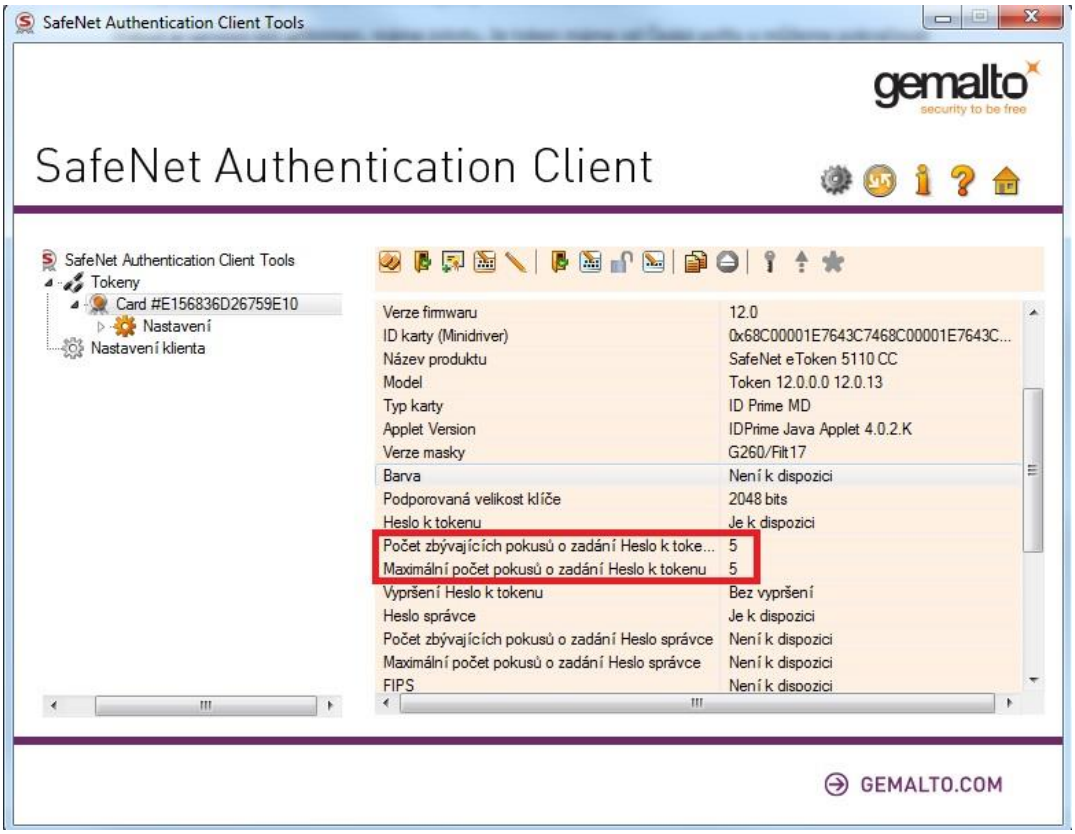
Pokud je servisní klíč přítomen, máme jistotu, že token je připravený pro vystavení žádosti o kvalifikovaný certifikát od České pošty a můžeme pokračovat kontrolou údajů v tokenu.

Ve stejném rozšířeném zobrazení, ale v pravé části, vidíme detailní informace o tokenu (název tokenu, kategorie tokenu, atd.) Zkontrolujeme počet zbývajících pokusů pro Heslo k tokenu, Digital Signature PIN a Digital Signature PUK. Řádky se jmenují:

Počet zbývajích pokusů o zadání – Heslo k tokenu (má být 5)

Digital Signature PIN retries remaining (má být 3)

Digital Signature PUK retries remaining (má být 3)


SafeNet Authentication Client Tools
gemalto
security to be free
SafeNet Authentication Client
SafeNet Authentication Client Tools
Tokeny
Card #E156836D26759E10
Nastavení
Nastavení klienta
Verze firmwaru 12.0
ID karty (Minidriver) 0x68C00001E7643C7468C00001E7643C...
Název produktu SafeNet eToken 5110 CC
Model Token 12.0.0.0 12.0.13
Typ karty ID Prime MD
Applet Version IDPrime Java Applet 4.0.2.K
Verze masky G260/Filt17
Barva Není k dispozici
Podporovaná velikost klíče 2048 bits
Heslo k tokenu Je k dispozici
Počet zbývajících pokusů o zadání Heslo k toke... 5
Maximální počet pokusů o zadání Heslo k tokenu 5
Vypršení Heslo k tokenu Bez vypršení
Heslo správce Je k dispozici
Počet zbývajících pokusů o zadání Heslo správce Není k dispozici
Maximální počet pokusů o zadání Heslo správce Není k dispozici
FIPS Není k dispozici
GEMALTO.COM

SafeNet Authentication Client Tools
gemalto
security to be free
SafeNet Authentication Client
SafeNet Authentication Client Tools
Tokeny
Card #E156836D26759E10
Nastavení
Nastavení klienta
Maximální počet pokusů o zadání Heslo k tokenu 5
Vypršení Heslo k tokenu Bez vypršení
Heslo správce Je k dispozici
Počet zbývajících pokusů o zadání Heslo správce Není k dispozici
Maximální počet pokusů o zadání Heslo správce Není k dispozici
FIPS Není k dispozici
Common Criteria (CC) CC EAL5+ / PP QSCD
Digital Signature PIN retries remaining 3
Digital Signature PIN maximum retries 3
Digital Signature PUK retries remaining 3
Digital Signature PUK maximum retries 3
Sign padding na tokenu Ano
RSM Není k dispozici
ECC Podporovaný
CSP Microsoft Base Smart Card Crypto Provider
KSP Microsoft Smart Card Key Storage Provider
GEMALTO.COM

Certifikační autorita PostSignum dodává k autentizačním předmětům vlastní sadu hesel, kterou důrazně doporučuje měnit:

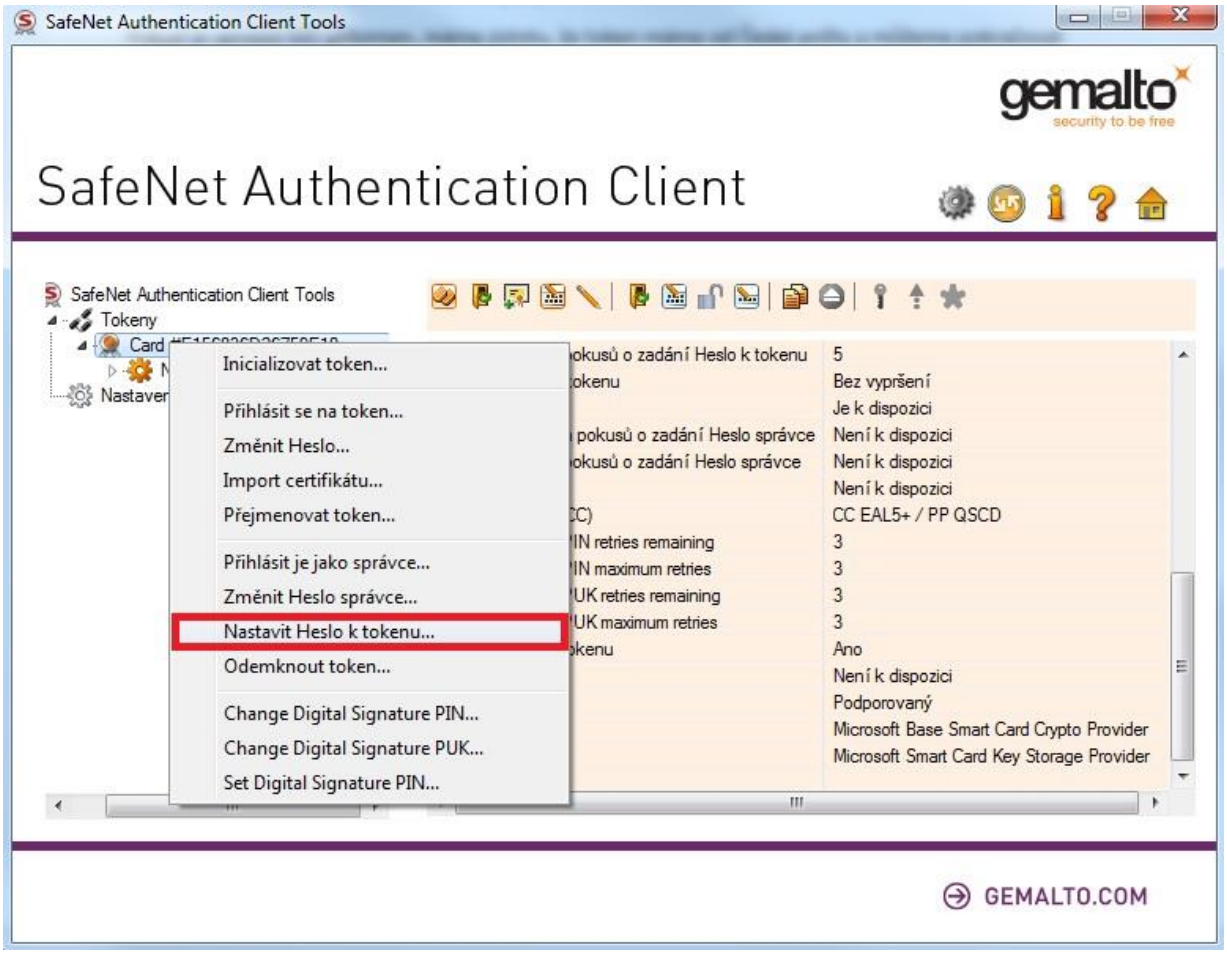
Heslo k tokenu	12345678
Administrátorské heslo	87654321
Digital Signature PIN	12345678
Digital Signature PUK	87654321

a) V případě zablokování Hesla k tokenu – počet 0

Pokud je číslo u „Počet zbývajících pokusů o zadání – Heslo k tokenu 0, podařilo se zablokovat token. Nicméně ho lze jednoduše odemknout za použití Administrátorského hesla.

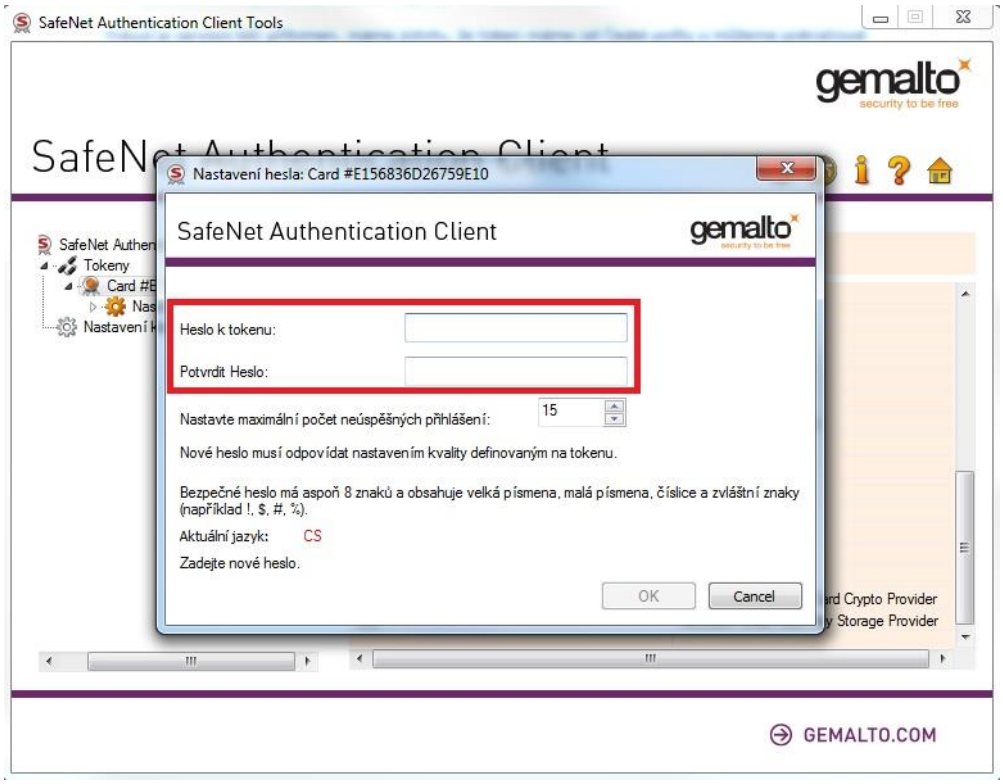
Odemkneme následujícím postupem:

1. V podrobném zobrazení (ozubené kolečko vpravo nahoře, při prvotním spuštění klienta) najdeme vlevo „strom“.
2. Pravým tlačítkem klikneme na název tokenu.
3. Vybereme možnost „Nastavit heslo k tokenu“.



4. Zadáme Administrátorské heslo.

5. Nastavíme nové heslo k tokenu.

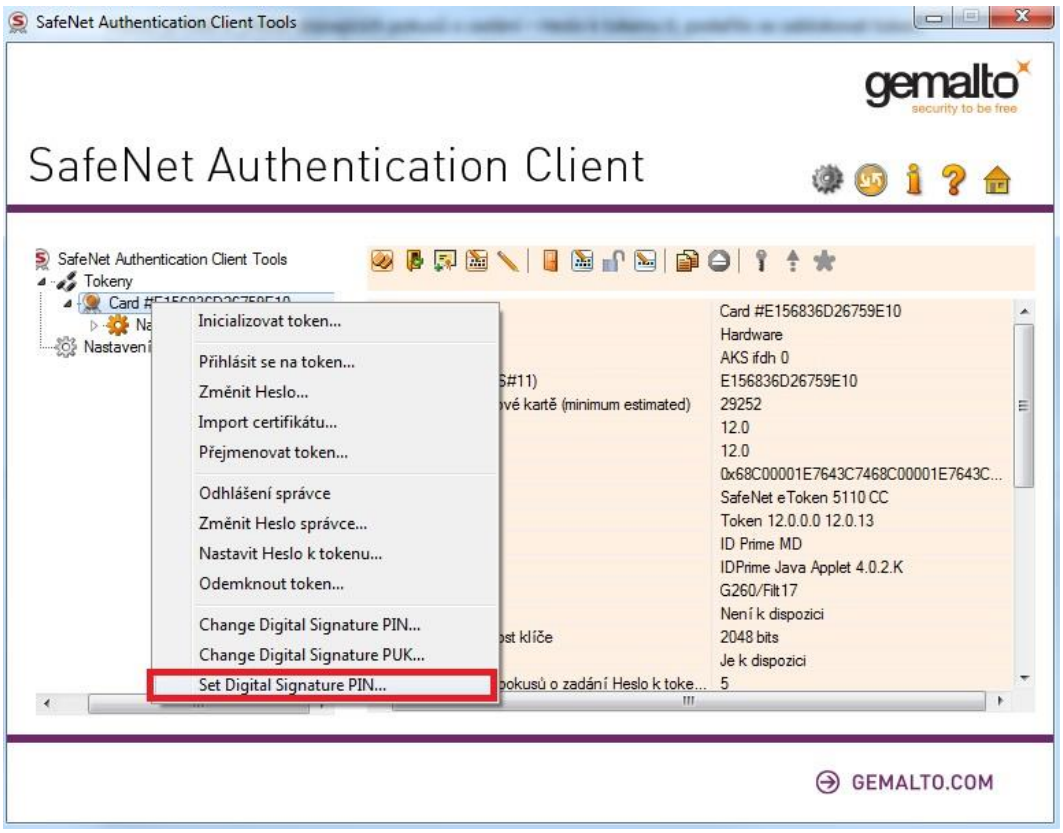


b) V případě zablokování Digital Signature PIN –počet 0

Pokud je číslo u Digital Signature PIN retries remaining 0, tak jsme 3x zadali špatný Digital Signature PIN a token je zamknut. I v tomto případě ho lze snadno odemknout, nyní za použití Digital Signature PUK.

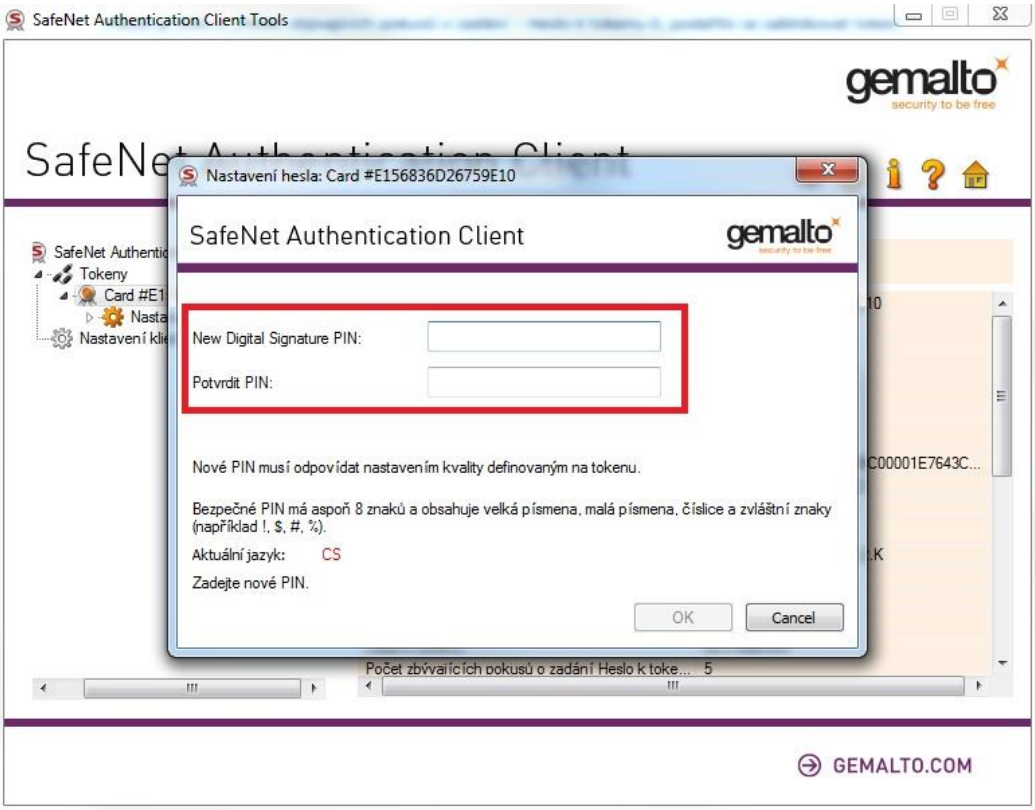
Odemkneme následujícím postupem:

1. V podrobném zobrazení (ozubené kolečko vpravo nahoře, při prvotním spuštění klienta) najdeme vlevo „strom“.
2. Pravým tlačítkem klikneme na název tokenu.
3. Vybereme možnost „Set Digital Signature PIN.



4. Zadáme Digital Signature PUK

5. Nastavíme nový Digital Signature PIN.



c) V případě zablokování Digital Signature PUK –počet 0

V tomto případě jsme se pokusili zadávat Digital Signature PUK a to 3x neúspěšně. Token není zamknut, nicméně jsme ztratili možnost si odemknout Digital Signature PIN v případě zablokování a přišli jsme o možnost token inicializovat (smazat a nastavit znovu). Pro inicializaci je Digital Signature PUK nezbytný.

Tokeny můžete dále používat, ale vystavujete se riziku zablokování PINu bez možnosti odemčení.

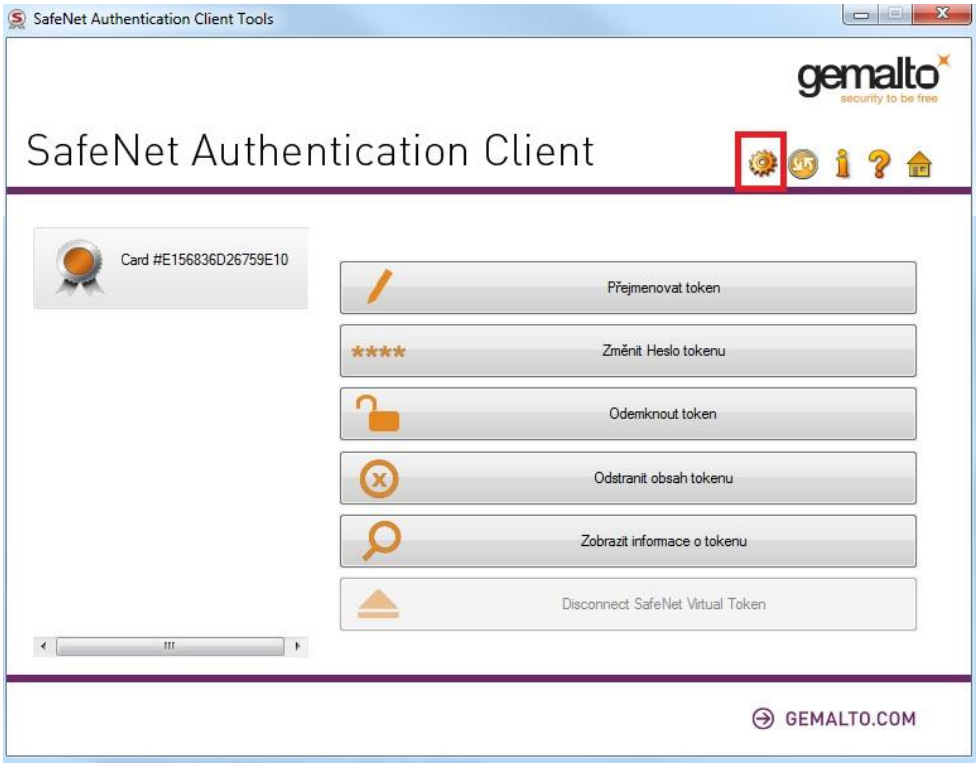
3) Token jsem pořídil/a od certifikační autority eIdentity

Certifikační autorita eIdentity generuje certifikáty na tokeny přímo. Není nutné kontrolovat přítomnost Servisního klíče.

Pro zjištění stavu, který údaj jsme si zablokovali, budeme postupovat následovně:

V pravém spodním rohu u hodin otevřete dvojitým poklepáním na ikonu svítícího „S“. Dostanete se do „Jednoduchého zobrazení“, kde vidíme možnosti jako: Přejmenovat token, Změnit heslo k tokenu, Odemknout token, atd.

Nyní zvolíme možnost rozšířeného zobrazení pomocí ikony ozubeného kola ve vrchní části obrazovky.

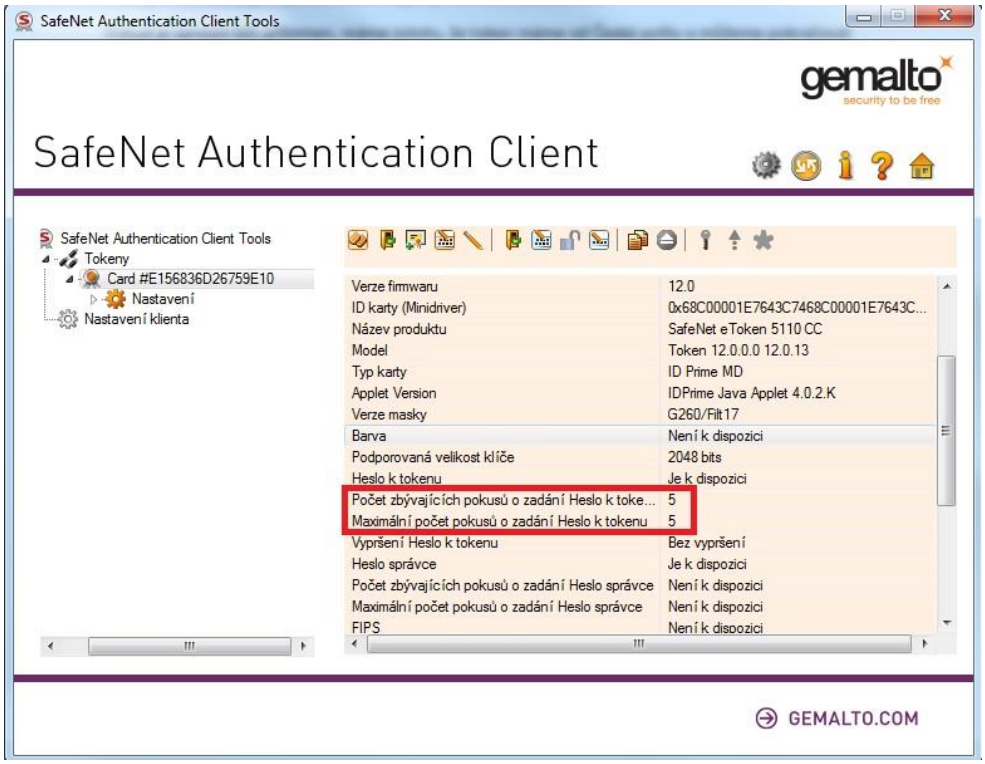


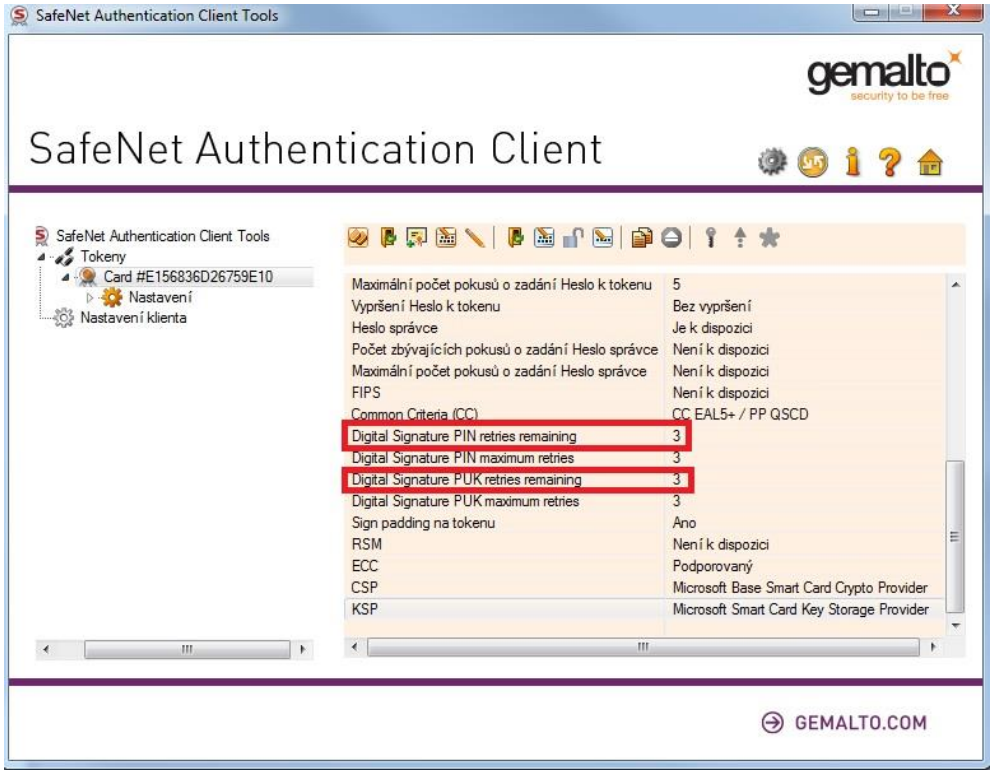
V pravé části vidíme detailní informace o tokenu (název tokenu, kategorie tokenu, atd.) Zkontrolujeme počet zbývajících pokusů pro Heslo k tokenu, Digital Signature PIN a Digital Signature PUK. Řádky se jmenují:

Počet zbývajích pokusů o zadání – Heslo k tokenu (má být 5)

Digital Signature PIN retries remaining (má být 3)

Digital Signature PUK retries remaining (má být 3)





V případě, že máte token od zprostředkovatelské společnosti, která Vám token zprovoznila, zeptejte se na aktuální přihlašovací údaje k tokenu. Certifikační autorita eIdentity dostává tokeny v továrním nastavení, pokud došlo ke změně přihlašovacích údajů Vámi či jinou firmou, tak následující tabulku továrního nastavení přihlašovacích údajů ignorujte.

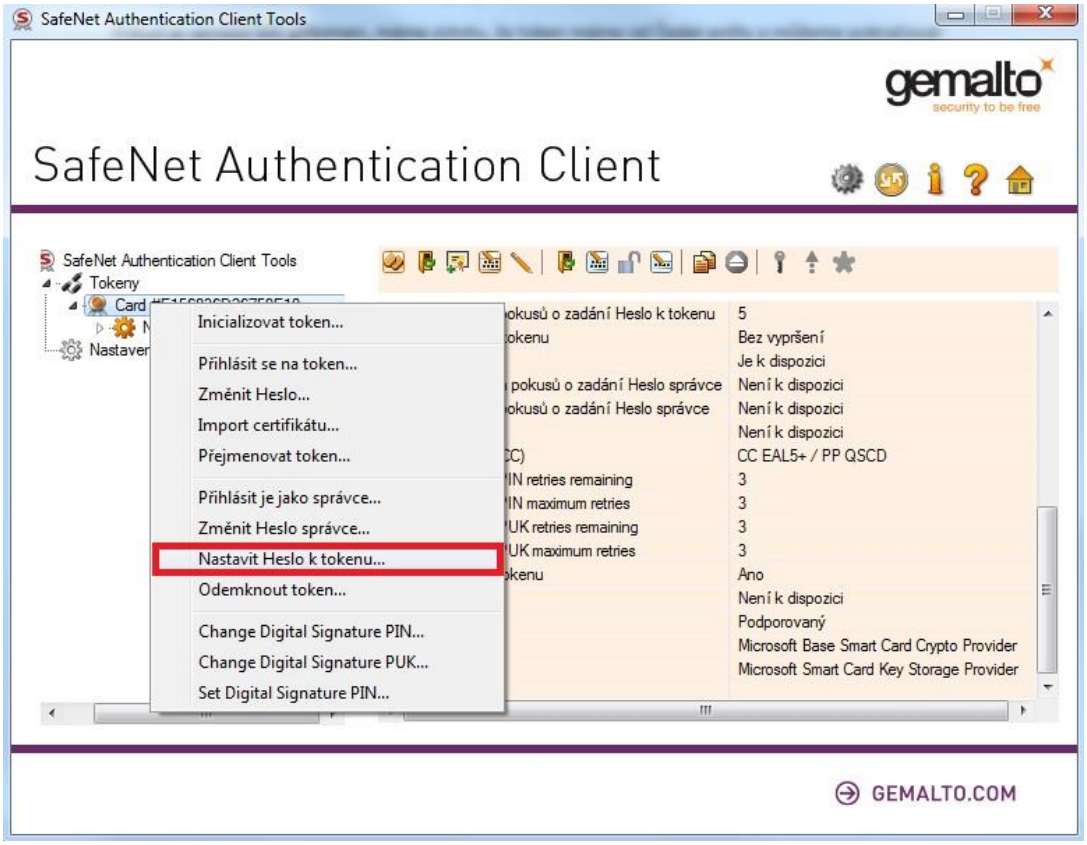
Heslo k tokenu	0000
Administrátorské heslo	0000000000000000000000000000000000000000000000000000
Digital Signature PIN	000000
Digital Signature PUK	000000

a) V případě zablokování Hesla k tokenu – počet 0

Pokud je číslo u „Počet zbývajících pokusů o zadání – Heslo k tokenu 0, podařilo se zablokovat token. Nicméně ho lze jednoduše odemknout za použití Administrátorského hesla.

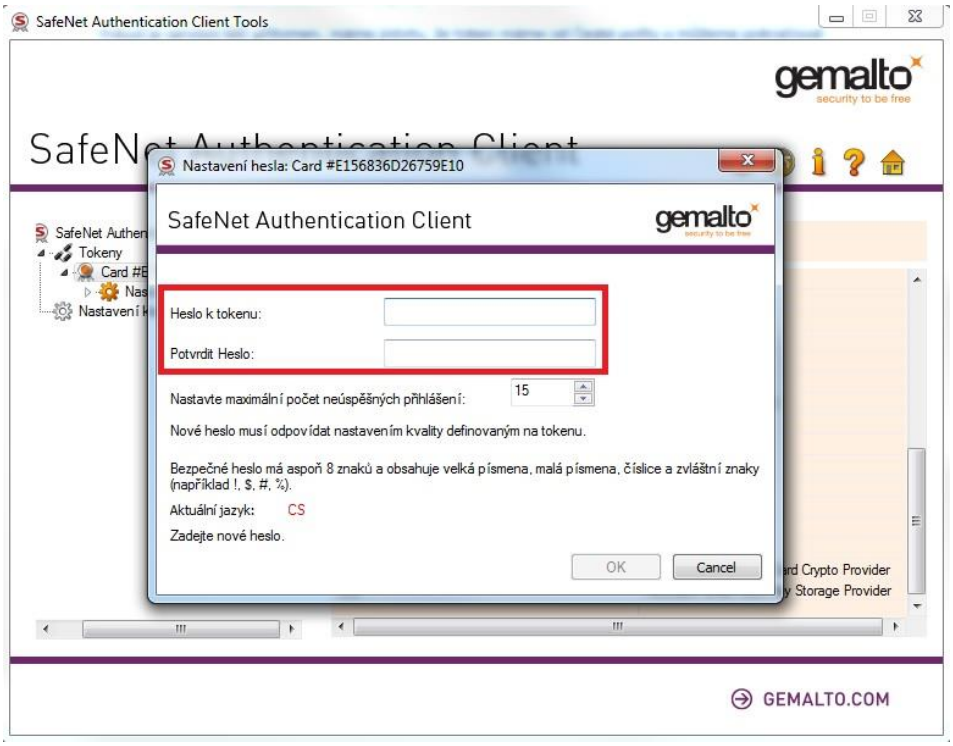
Odemkneme následujícím postupem:

1. V podrobném zobrazení (ozubené kolečko vpravo nahoře, při prvotním spuštění klienta) najdeme vlevo „strom“.
2. Pravým tlačítkem klikneme na název tokenu.
3. Vybereme možnost „Nastavit heslo k tokenu“.



4. Zadáme Administrátorské heslo.

5. Nastavíme nové heslo k tokenu.

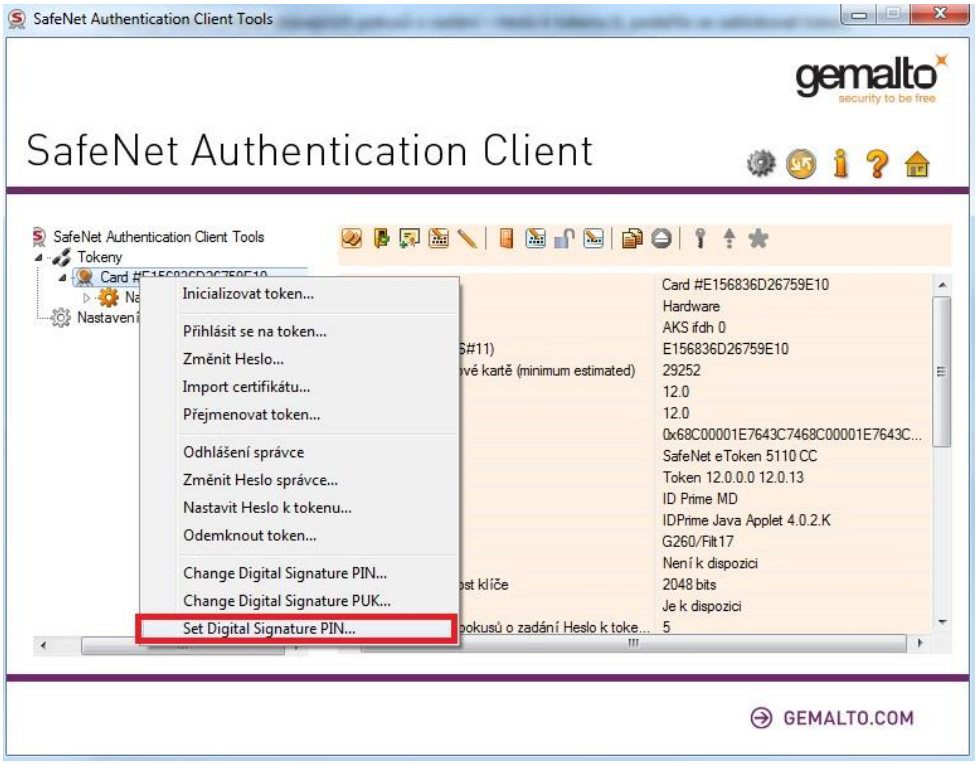


b) V případě zablokování Digital Signature PIN – počet 0

Pokud je číslo u Digital Signature PIN retries remaining 0, tak jsme 3x zadali špatný Digital Signature PIN a token je zamknut. I v tomto případě ho lze snadno odemknout, nyní za použití Digital Signature PUK.

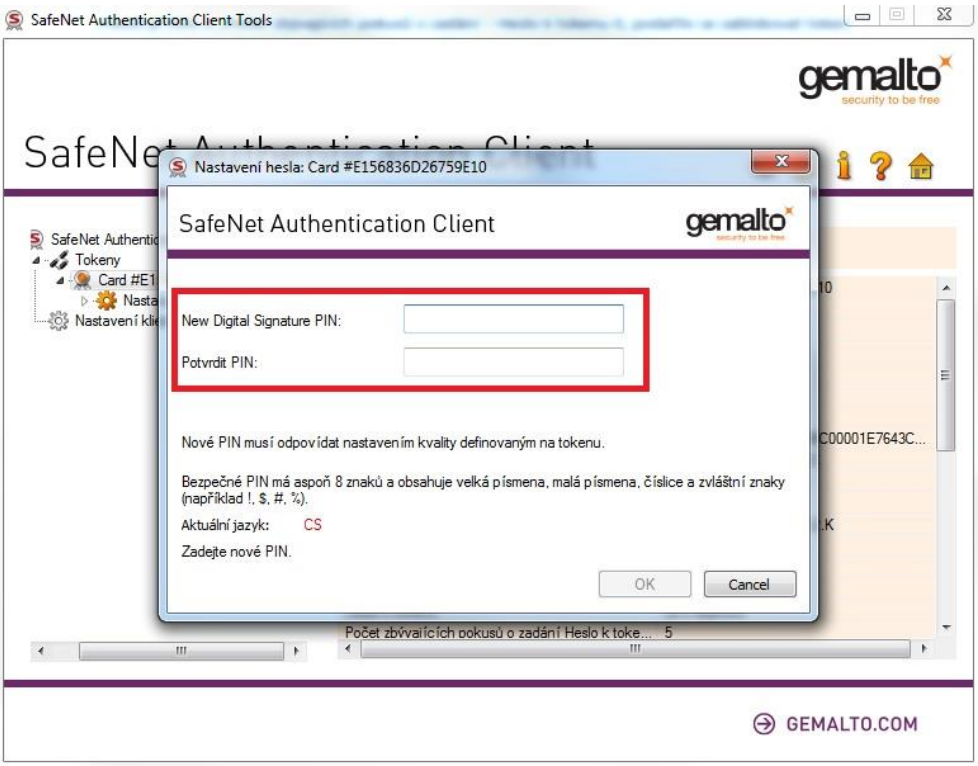
Odemkneme následujícím postupem:

1. V podrobném zobrazení (ozubené kolečko vpravo nahoře, při prvotním spuštění klienta) najdeme vlevo „strom“.
2. Pravým tlačítkem klikneme na název tokenu.
3. Vybereme možnost „Set Digital Signature PIN.



4. Zadáme Digital Signature PUK

5. Nastavíme nový Digital Signature PIN.



c) V případě zablokování Digital Signature PUK – počet 0

V tomto případě jsme se pokusili zadávat Digital Signature PUK a to 3x neúspěšně. Token není zamknut, nicméně jsme ztratili možnost si odemknout Digital Signature PIN v případě zablokování a přišli jsme o možnost token inicializovat (smazat a nastavit znovu). Pro inicializaci je Digital Signature PUK nezbytný.

Tokeny můžete dále používat, ale vystavujete se riziku zablokování PINu bez možnosti odemčení.