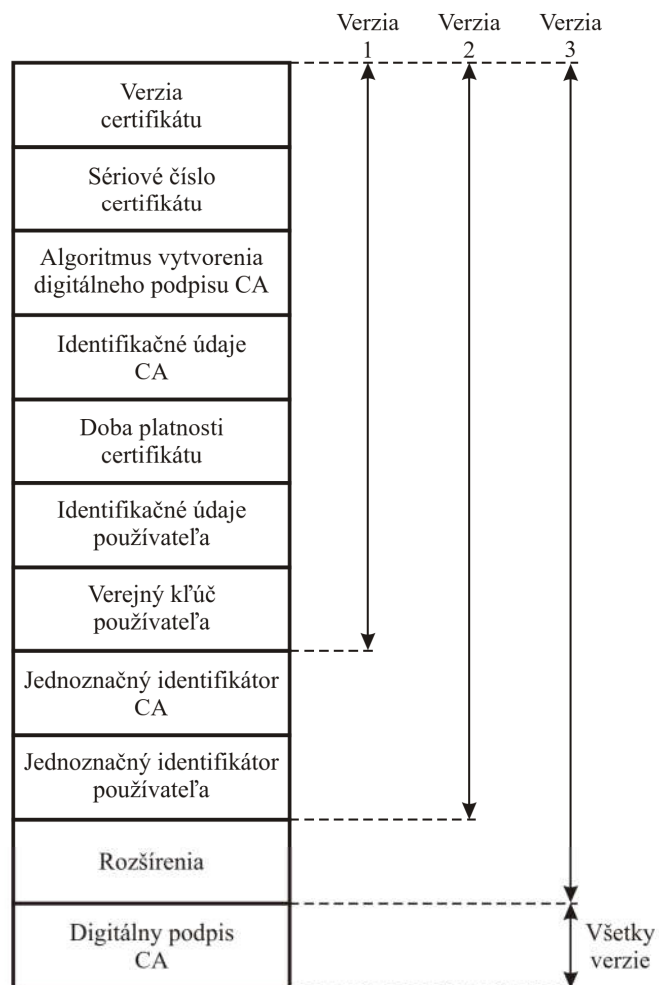


## Certifikáty podľa odporúčania X.509

**Formáty certifikátov** určuje odporúčanie ITU–T X.509, ktoré je časťou odporúčania X.500. Odporúčanie X.509 definuje tiež **autentizačné protokoly**, ktoré sa používajú v rôznych **typoch sietí** a v rôznych **aplikáciách sieťovej bezpečnosti**.

Všeobecný formát certifikátov podľa odporúčania X.509 je uvedený na *Obr. 8.5* a obsahuje tieto položky:



Obr. 8.5 Formáty certifikátov podľa odporúčania X.509

**Verzia certifikátu** (Version) udáva jednu z troch verzií certifikátu (1, 2 alebo 3), ktoré sa líšia celkovým počtom položiek certifikátu a sú definované v odporúčaní X.509.

**Sériové číslo certifikátu** (Serial number) je definované ako celé nezáporné číslo, ktoré je pridelené na označenie daného certifikátu certifikačnou autoritou (CA). Sériové číslo musí byť v rámci danej certifikačnej autority jednoznačné, t. j. certifikačná autorita nesmie vydať dva certifikáty s rovnakým sériovým číslom.

**Algoritmus vytvorenia digitálneho podpisu CA** (Signature algorithm identifier) je položka, ktorá obsahuje informácie o algoritme, ktorý bol použitý na podpis certifikátu a príslušné parametre tohto podpisu.

**Identifikačné údaje CA** (Issuer) je položka, ktorá obsahuje meno CA v zmysle odporúčania X.500, ktorá vydala certifikát. Certifikačná autorita CA by mala mať jednoznačnú identifikáciu, t. j. jedinečné meno v rámci všetkých certifikačných autorít.

**Doba platnosti certifikátu** (Period of validity) je položka určujúca platnosť certifikátu, obsahuje dva časy, t. j. odkedy a dokedy certifikát platí.

**Identifikačné údaje používateľa** (Subject name) je položka, ktorá obsahuje jedinečné meno subjektu, ktorému je certifikát vydaný, t. j. obsahuje identifikáciu držiteľa certifikátu, ktorý je vlastníkom súkromného kľúča zodpovedajúceho certifikovanému verejnému kľúču.

**Verejný kľúč používateľa** (Subject's public-key) je položka, ktorá obsahuje dve položky a to identifikátor algoritmu, pre ktorý je verejný kľúč určený a samotný verejný kľúč.

Odporúčanie X.509 vo verzii 2 definuje ďalšie dve položky certifikátu. Sú to:

**Jednoznačný identifikátor CA** (Issuer unique identifier) je položka určená pre jednoznačnú identifikáciu CA v prípade, že meno CA v položke Identifikačné údaje CA (Issuer) bolo použité v rôznych CA, resp. keď táto položka nepostačuje na jednoznačnú identifikáciu CA.

**Jednoznačný identifikátor používateľa** (Subject unique identifier) je obdobná položka ako predošlá a týka sa používateľa, t. j. držiteľa certifikátu.

Položka **Rozšírenie** (Extension) definovaná vo verzii 3 obsahuje ďalšie informácie o kľúčoch CA a používateľa, o identifikátoroch CA a používateľa ako aj o certifikačnej politike a obmedzeniach týkajúcich sa vydávania certifikátov.

**Digitálny podpis CA** (Signature of CA) obsahuje hašovací kód<sup>(1)</sup> ostatných položiek certifikátu, ktorý je zašifrovaný súkromným kľúčom CA.