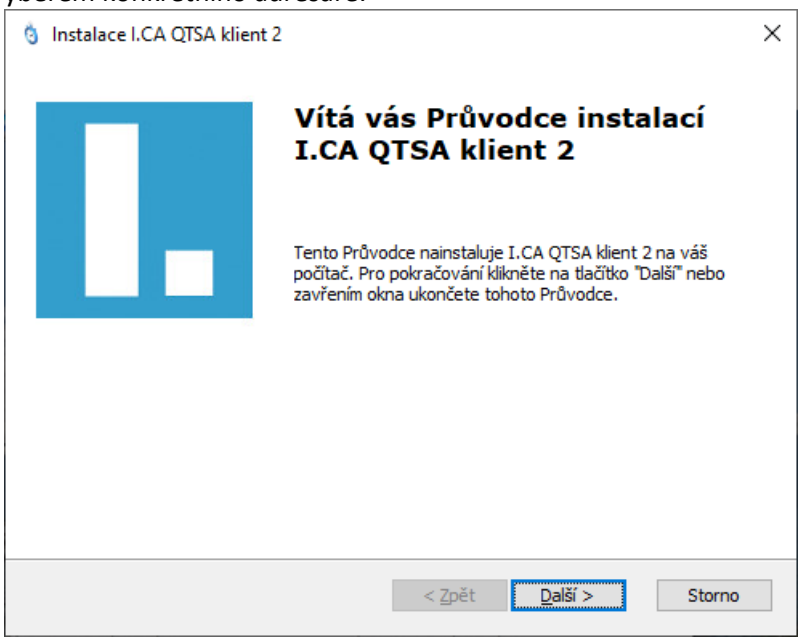
Aplikace I.CA QTSAklient2 verze 1.1.0.0 a vyšší

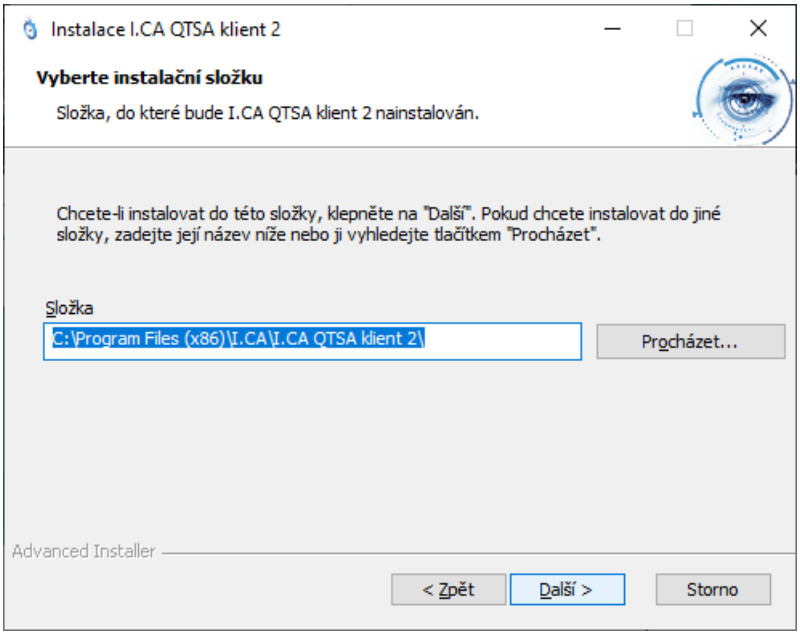
Aplikace QTSA klient 2 umožňuje získání kvalifikovaného elektronického časového razítka (vytvoření žádosti o časové razítko dle Politiky služby) z časové autority První certifikační autority, a. s. (I.CA). Časové razítko je možné připojit ke konkrétnímu elektronickému dokumentu resp. souboru a datům. Vhodná je pro situace, kdy jsou časová razítka požadována jednotlivě konkrétním uživatelem. Aplikaci lze používat, pouze pokud máte službu časové autority sjednánu s I.CA a nastaven aktivní přístup k této službě (TSA/ATSA). QTSA klient 2 vyžaduje ke své činnosti on-line připojení k internetu.

1.1 Instalace

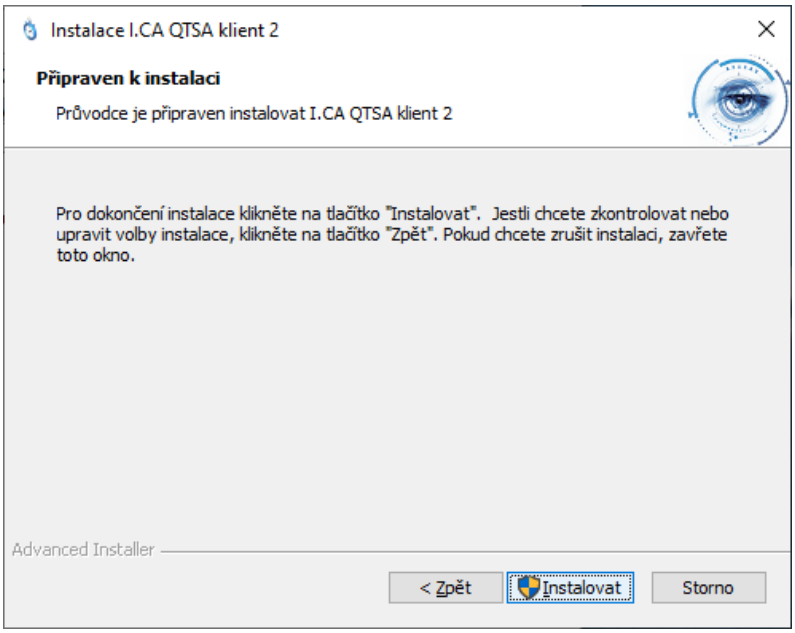
Rozbalte soubor QTSAKlient2Setup.zip do nového adresáře např. QTSA_klient2 – spusťte soubor QTSAKlient2Setup.exe. Doporučujeme instalovat jako „správce“.

Průvodce instalací je uživatelsky intuitivní, potvrďte přednastavené volby, případně můžete změnit uložení instalace, výběrem konkrétního adresáře.

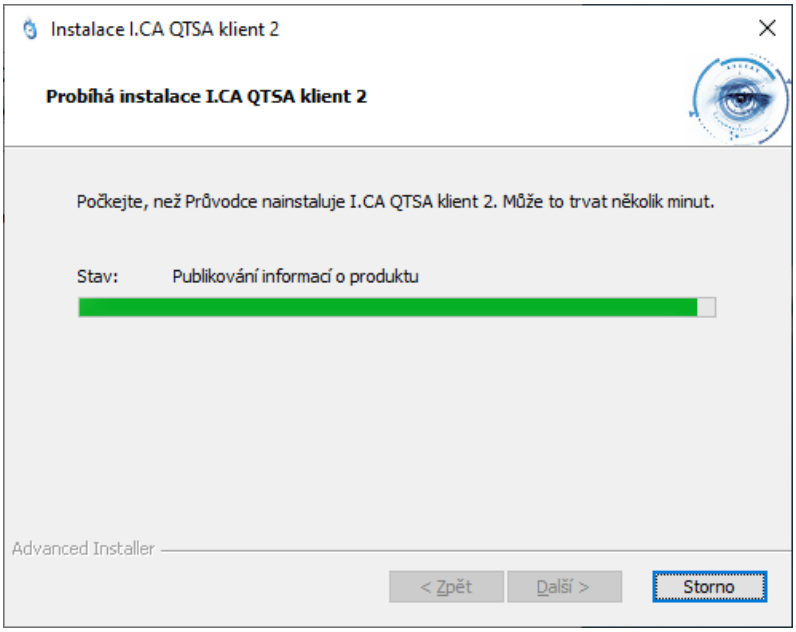




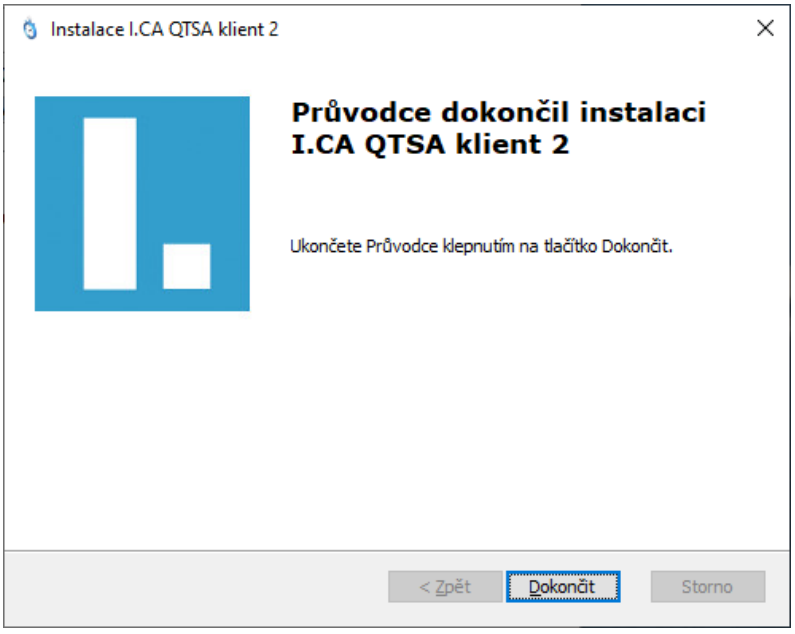
Potvrzením tlačítka „Instalovat“ se spustí instalace.



Průběh je možné sledovat na obrazovce.



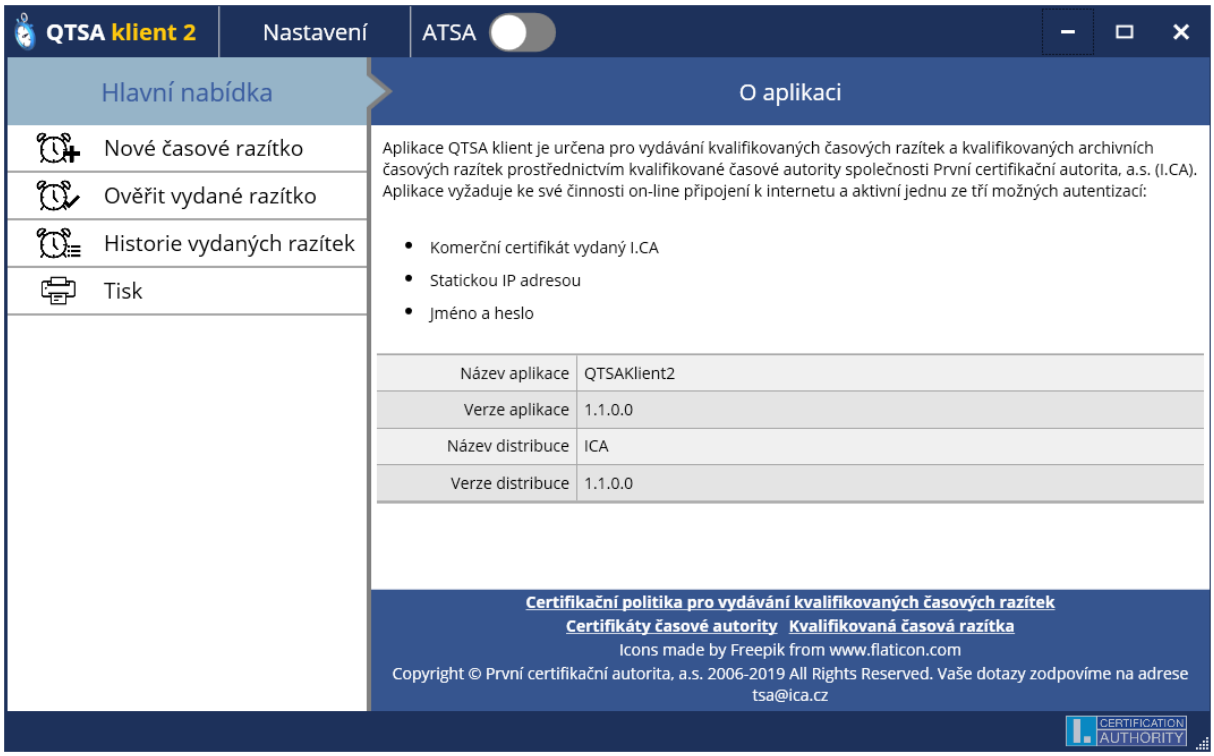
Úspěšné dokončení instalace potvrdíte tlačítkem „Dokončit“.



1.2 Spuštění aplikace

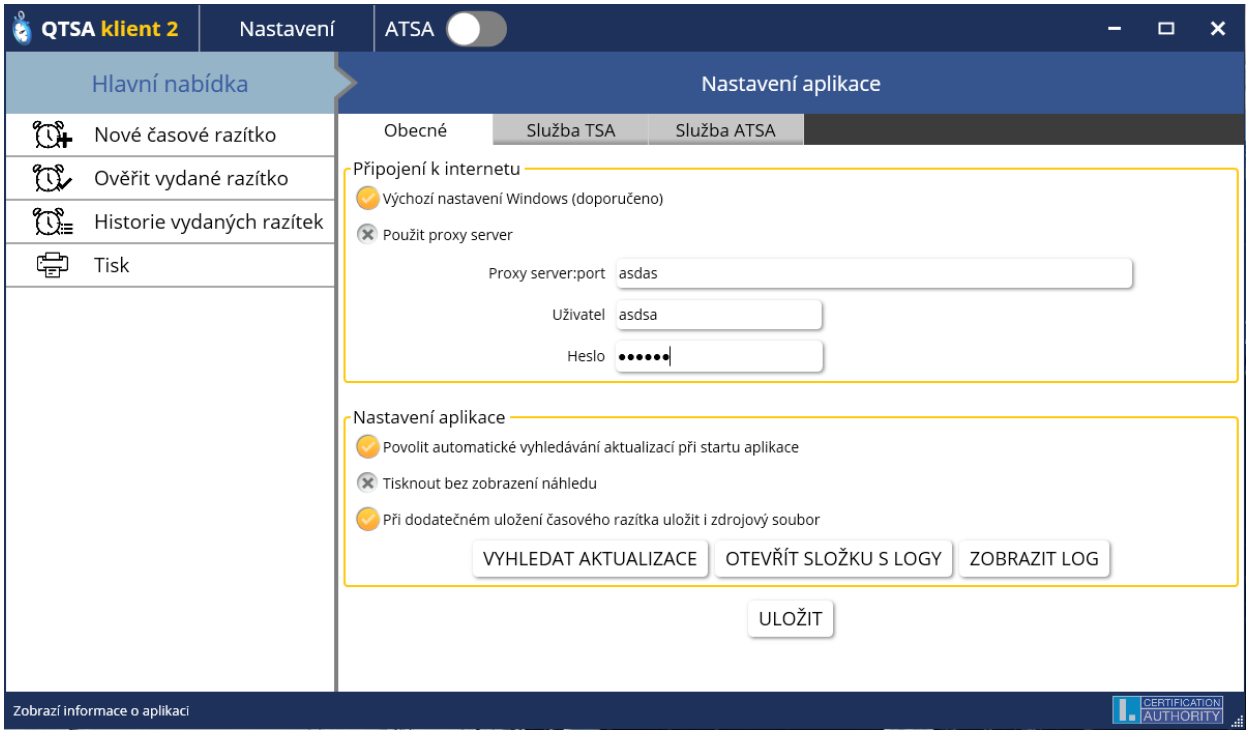
Po spuštění aplikace se zobrazí hlavní okno skládající se následujících částí:

- Informace o aplikaci, kde lze nalézt informace o aktuální verzi aplikace
- Hlavní nabídka odkud se lze navigovat na jednotlivé funkce aplikace (vytvoření časového razítka atd.)
- Horní menu, odkud lze přejít do nastavení, aktivovat režim ATSA (archivní časová razítka, viz. https://www.ica.cz/archivni-elektronicka-casova-razitka)



1.3 Nastavení aplikace

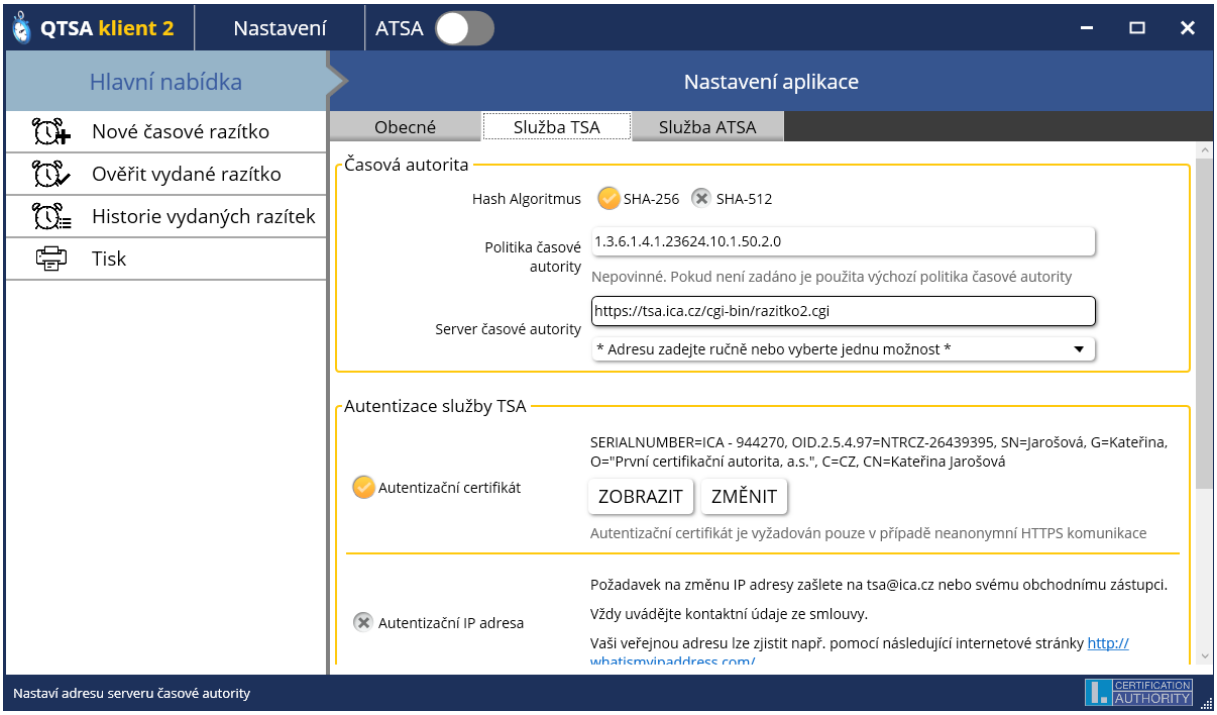
- Nastavení aplikace lze provést pomocí tlačítka **Nastavení** umístěné v horním menu aplikace.
- Obrazovka nastavení se skládá ze tří částí:
    - Obecné – zde lze spravovat připojení k internetu a automatické vyhledávání aktualizací
        - Nastavení Proxy – umožňuje manuální nastavení Proxy serveru
        - Automatické vyhledávání aktualizací – umožní aplikaci automaticky se po spuštění dotazovat, zda nejsou dostupné aktualizace aplikace
        - Kopírování zdrojového souboru při dodatečném ukládání časového razítka – při dodatečném ukládání časového razítka nebo tokenu časového razítka (viz kapitola **1.5 Obsah detailního pohledu**) aplikace zkopíruje do adresáře (kam se časové razítko dodatečně uloží) také zdrojový soubor, ke kterému bylo časové razítko vytvořeno.



- Služba TSA – umožňuje parametrizovat službu vydání časových razítek (výchozí hash algoritmus, politiku časové autority, server časové autority a způsob autentizace)
- Služba ATSA – umožňuje parametrizovat službu vydání archivních časových razítek (výchozí hash algoritmus, politiku časové autority, server časové autority a způsob autentizace)

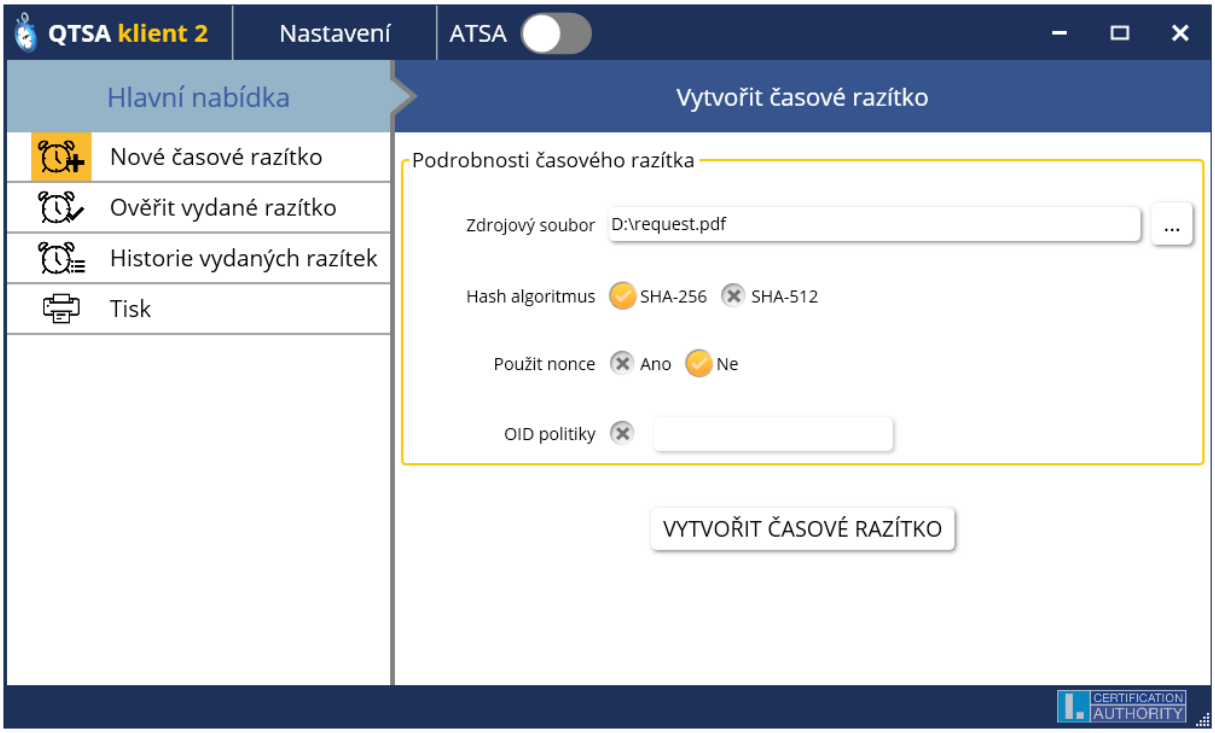
- Nastavení spojení s časovou autoritou TSA2/ATSA2, v případě nefunkčnosti níže uvedených URL si vyžádejte aktuální údaje na e-mailové adrese: tsa@ica.cz nebo podpora@ica.cz.

služba	autorizace	typ spojení	URL
TSA2	certifikátem	neanonymní HTTPS	https://tsa.ica.cz/cgi-bin/razitko2.cgi
TSA2 BASE	jménem a heslem	neanonymní HTTPS	https://tsabase.ica.cz/cgi-bin/razitko_base2.cgi
TSA2 BASE	jménem a heslem	HTTP	http://tsabase.ica.cz/cgi-bin/razitko_base2.cgi
TSA2 IP	IP adresou	HTTP	http://tsabase.ica.cz/cgi-bin/razitko_ip2.cgi
ATSA2	certifikátem	neanonymní HTTPS	https://tsa.ica.cz/cgi-bin/razitko_atsa2.cgi
ATSA2	jménem a heslem	neanonymní HTTPS	https://tsabase.ica.cz/cgi-bin/razitko_atsa_base2.cgi
ATSA2	jménem a heslem	HTTP	http://tsabase.ica.cz/cgi-bin/razitko_atsa_base2.cgi
ATSA2	IP adresou	HTTP	http://tsabase.ica.cz/cgi-bin/razitko_atsa_ip2.cgi
OID politika	1.3.6.1.4.1.23624.10.1.50.2.0		

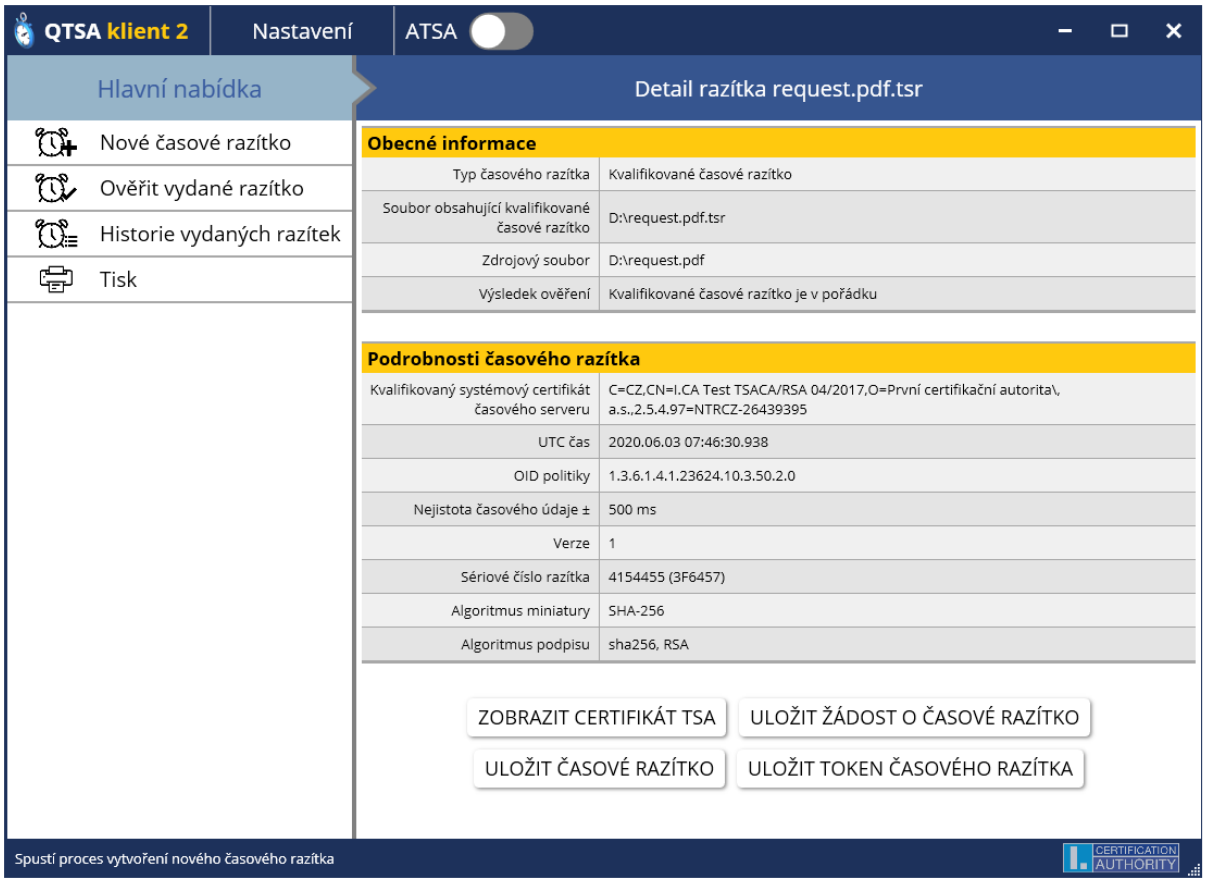


1.4 Vydání časového razítka

- Kliknutím na volbu (tlačítko) **Nové časové razítko**  se zobrazí průvodce pro vydání časového razítka
- V zobrazeném okně vyberte zdrojový soubor (soubor, ke kterému chcete vydat časové razítko). Po výběru zdrojového souboru klikněte na tlačítko **Otevřít**.
- V aplikaci se zobrazí okno, ve kterém si lze nastavit parametry žádosti o časové razítko (např. použitý Hash algoritmus, výběr vlastní OID politiky atd.)
- Stiskem tlačítka „Vytvořit časové razítko“ se, pokud je vše v pořádku, program pokusí navázat zabezpečené On-line spojení se serverem TSA. Pro vydání časového razítka je nutné mít nastavené parametry spojení, které je možno nastavit v obrazovce **Nastavení**. (viz. kapitola 1.1 Nastavení aplikace). Název souboru přijatého časového razítka aplikace přednastaví na původní název souboru s příponou „.tst“.
- Přijaté časové razítko je poté vloženo do **Historie vydaných razítek** a údaje o razítku se zobrazí v detailním pohledu vpravo.
- Pokud je aktivován režim ATSA, průběh vytvoření časového razítka je stejný, jen místo vytvoření kvalifikovaného časového razítka dojde k vytvoření archivního kvalifikovaného časového razítka.



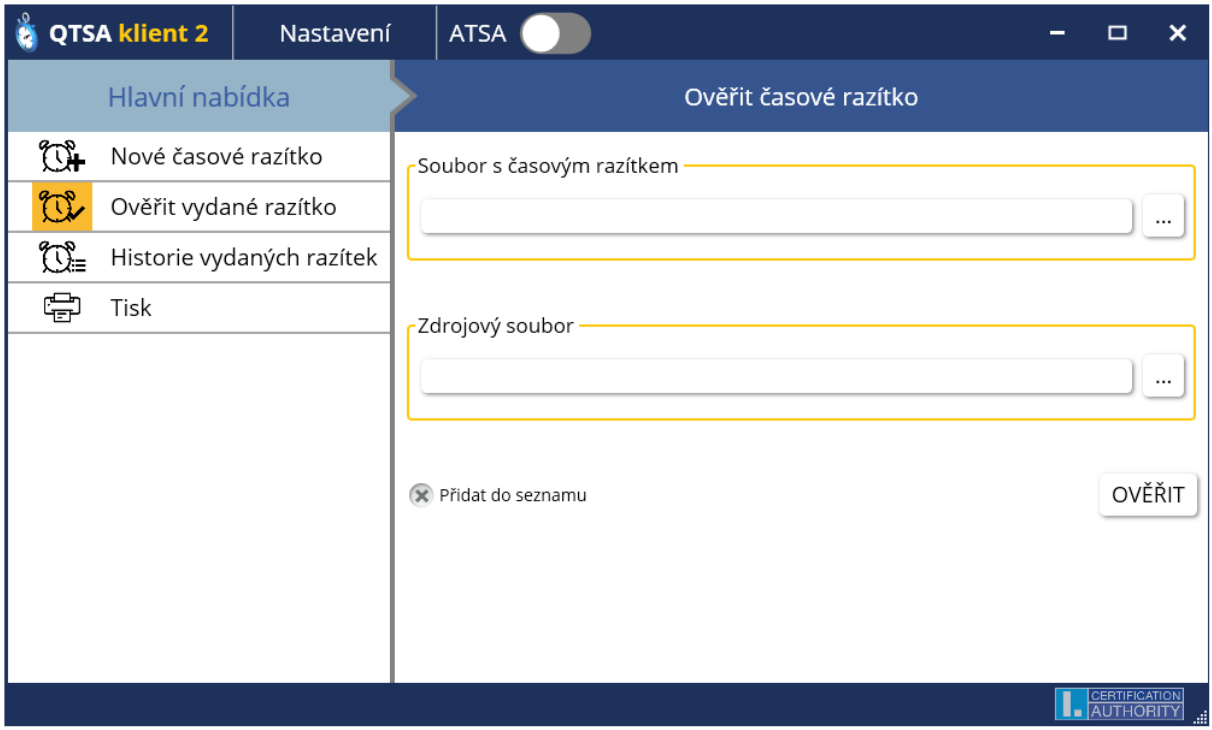
1.5 Obsah detailního pohledu



- Sekce **Obecné informace** zobrazuje souhrnný přehled o dvojici časové razítko – zdrojový dokument. Dále obsahuje informace o výsledku kontroly struktury časového razítka, výsledku kontroly digitálního podpisu razítka a shody miniatury zdrojového souboru a miniatury obsažené v časovém razítku a souhrnnou informaci o výsledku kontrol.
- Sekce **Podrobnosti časového razítka** obsahuje údaje o časovém razítku
- V detailu vydaného razítka si lze pomocí tlačítka zobrazit informace o certifikátu časové autority. Dále lze dodatečně uložit žádost o časové razítko, časové razítko nebo token časového razítka

1.6 Ověření časového razítka

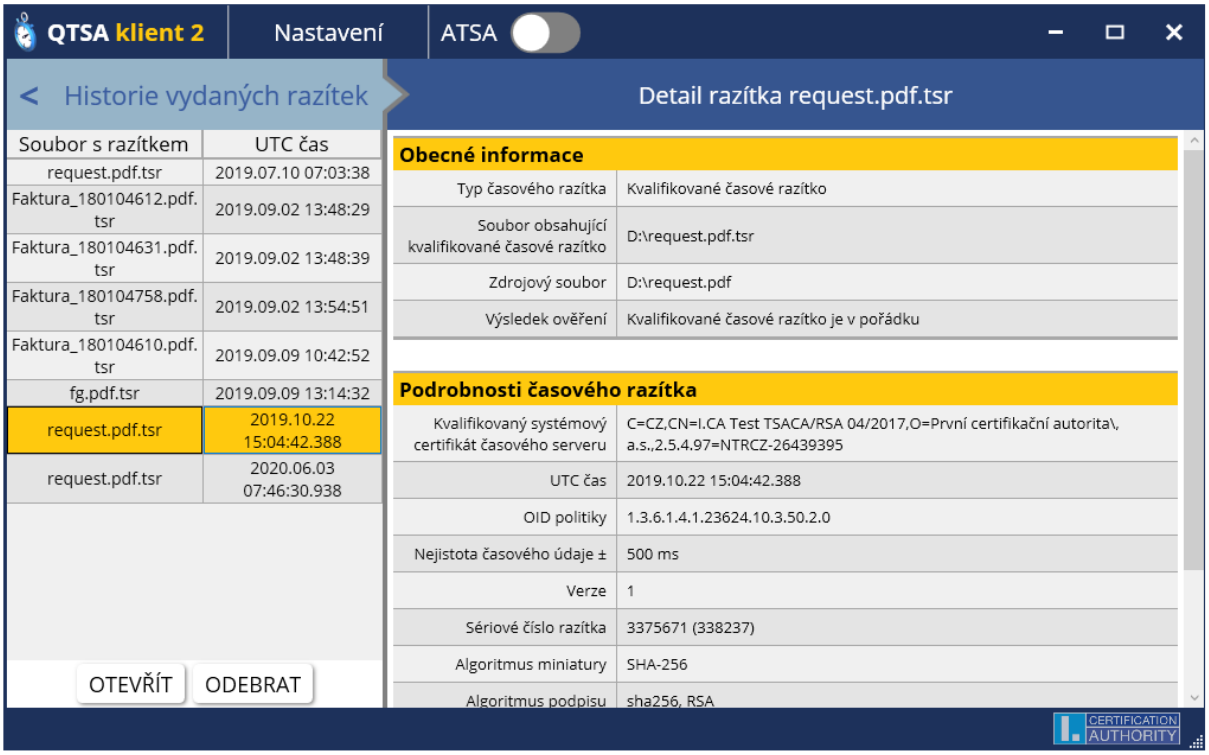
- Kliknutím na tlačítko **Ověřit vydané razítko**  Ověřit vydané razítko se zobrazí průvodce pro ověření existujícího časového razítka



- V sekci **Soubor s časovým razítkem** lze pomocí tlačítka **…** vybrat pomocí dialogu soubor s časovým razítkem. Po stisku tlačítka **Otevřít** v dialogu se aplikace pokusí automaticky vyhledat Zdrojový soubor časového razítka. Pokud zdrojový soubor aplikace nenalezne je potřeba soubor najít manuálně pomocí tlačítka **…** v sekci **Zdrojový soubor**. Po výběru obou souborů klikněte na tlačítko **Ověřit**
- Pokud vyberete existující soubor a kliknete na tlačítko **Ověřit** je provedena kontrola miniatur (hashe) tohoto souboru a miniatury z časového razítka a pokud jsou miniatury shodné (jedná se o platný pár dokument – časové razítko) je zobrazena zpráva o úspěšném ověření razítka.
- Ověřované časové razítko je možné vložit do **Historie vydaných razítek** a zobrazit jeho detail pomocí zaškrtávacího políčka **Přidat do seznamu**.

1.7 Historie vydaných razítek

- K seznamu vydaných razítek lze přistoupit pomocí tlačítka **Historie vydaných razítek**
  Historie vydaných razítek
- V levé části obrazovky je zobrazen seznam vydaných razítek a po vybrání konkrétního časového razítka ze seznamu je zobrazen jeho detail.
- Do seznamu lze přidávat existující časové razítka pomocí tlačítka **Otevřít**
- Ze seznamu lze vybrané časové razítko odstranit pomocí tlačítka **Odstranit** (odstraní se pouze z historie vydaných časových razítek, soubor časového razítka v počítači zůstane).



Další informace jsou k dispozici v Nápovědě aplikace, případné jakékoliv dotazy Vám zodpovíme na e-mailových adresách: tsa@ica.cz nebo podpora@ica.cz.