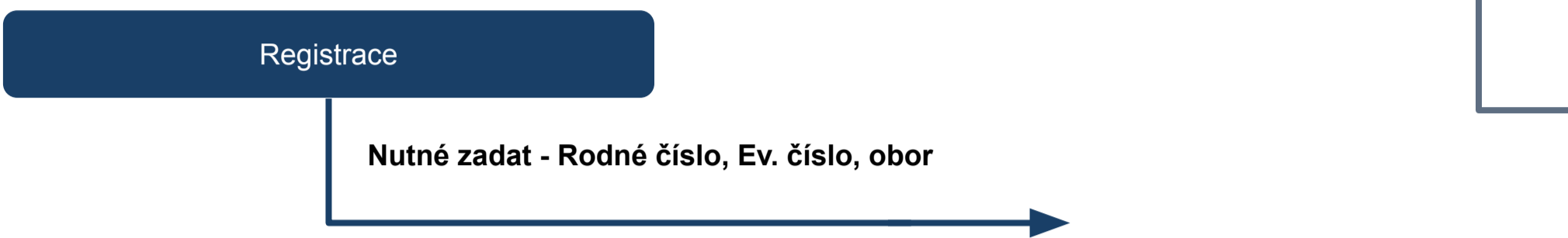
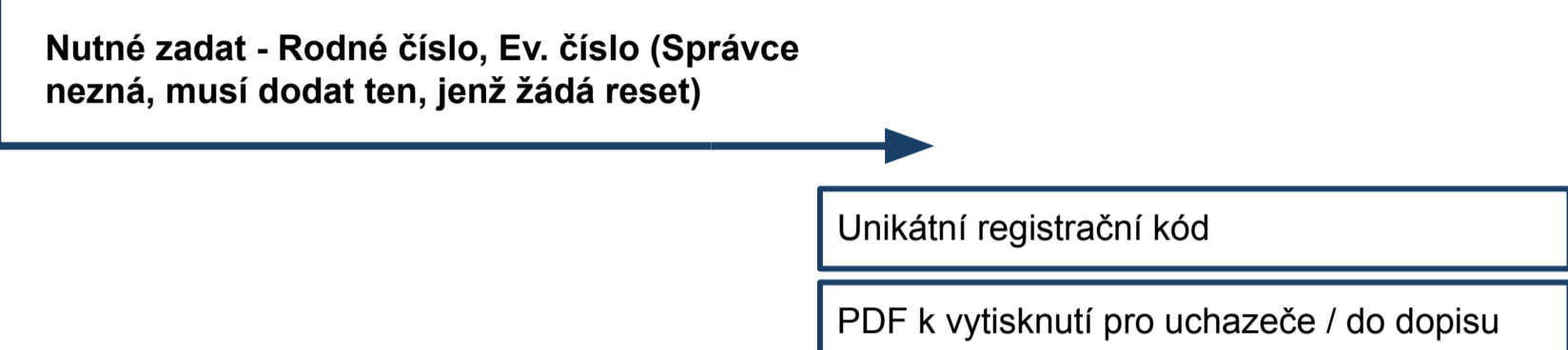


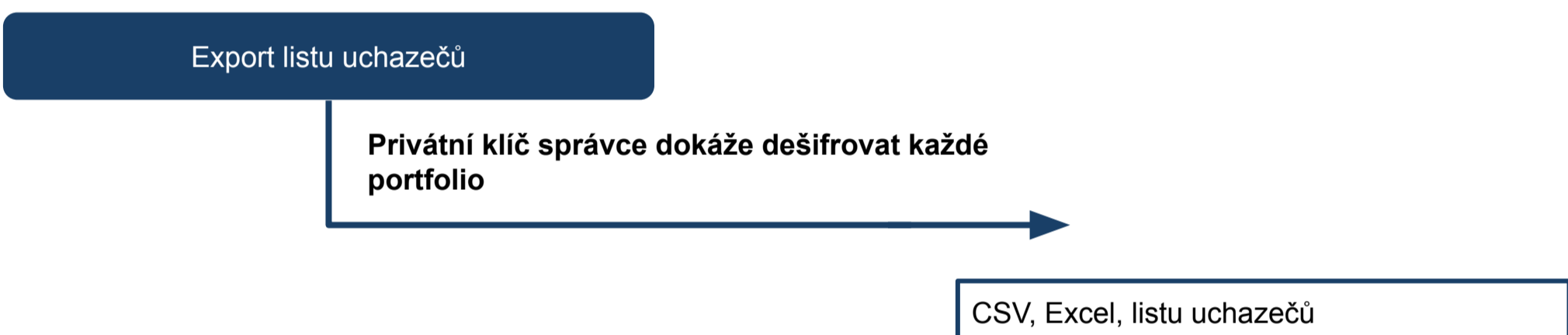
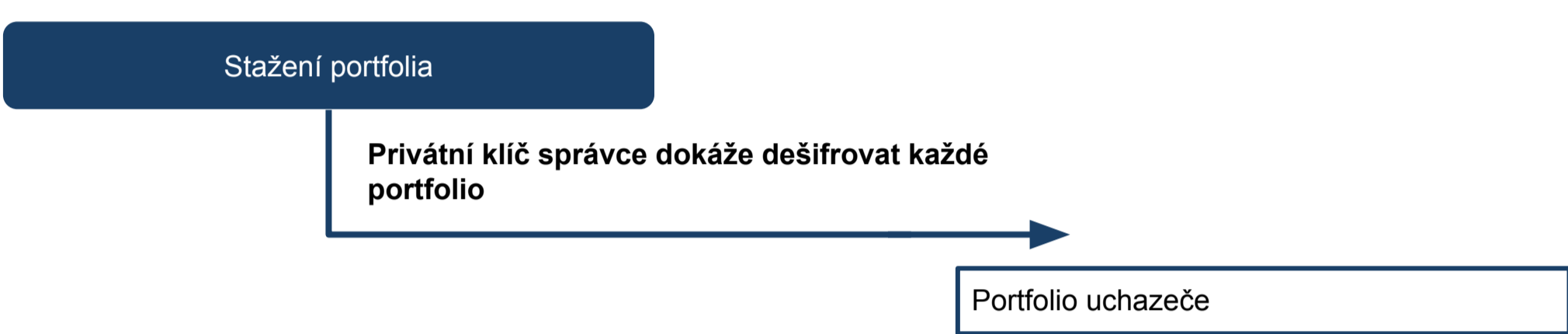
Pravomoce správce (Odevzdávání přihlášek)



Znovuvytvoření (reset) kódu



Pravomoce správce (Komise)



Garance bezpečnosti

Všechny důležitá data na disku a v databázi jsou šifrovány veřejným klíčem správce a případně veřejným klíčem uchazeče. Ani přímý přístup na všechny školní servery, mimo jiné například přes jiný zranitelný školní produkt, by ani v nejmenším případě neohrozil zašifrované údaje. Myslíme si, že s touto architekturou se bude jednat, co se týče manipulace s osobními údaji, o nejbezpečnější aplikaci v portfoliu SSPŠaG.

Únik privátního klíče správce bez získání kompletního přístupu na servery SSPŠaG (Vysoce nepravděpodobné 😊), neznamená žádné bezpečnostní riziko. V případě incidentu tohoto druhu by se vygenerovaly nové kryptografické klíče a data na serveru by se rešifrovaly.

Privátní klíče server zná pouze v podobě bezpečné šifry AES a jejich výpis je možný pouze po zadání hesla, které zná pouze uchazeč, či správce.

Garance uchování dat

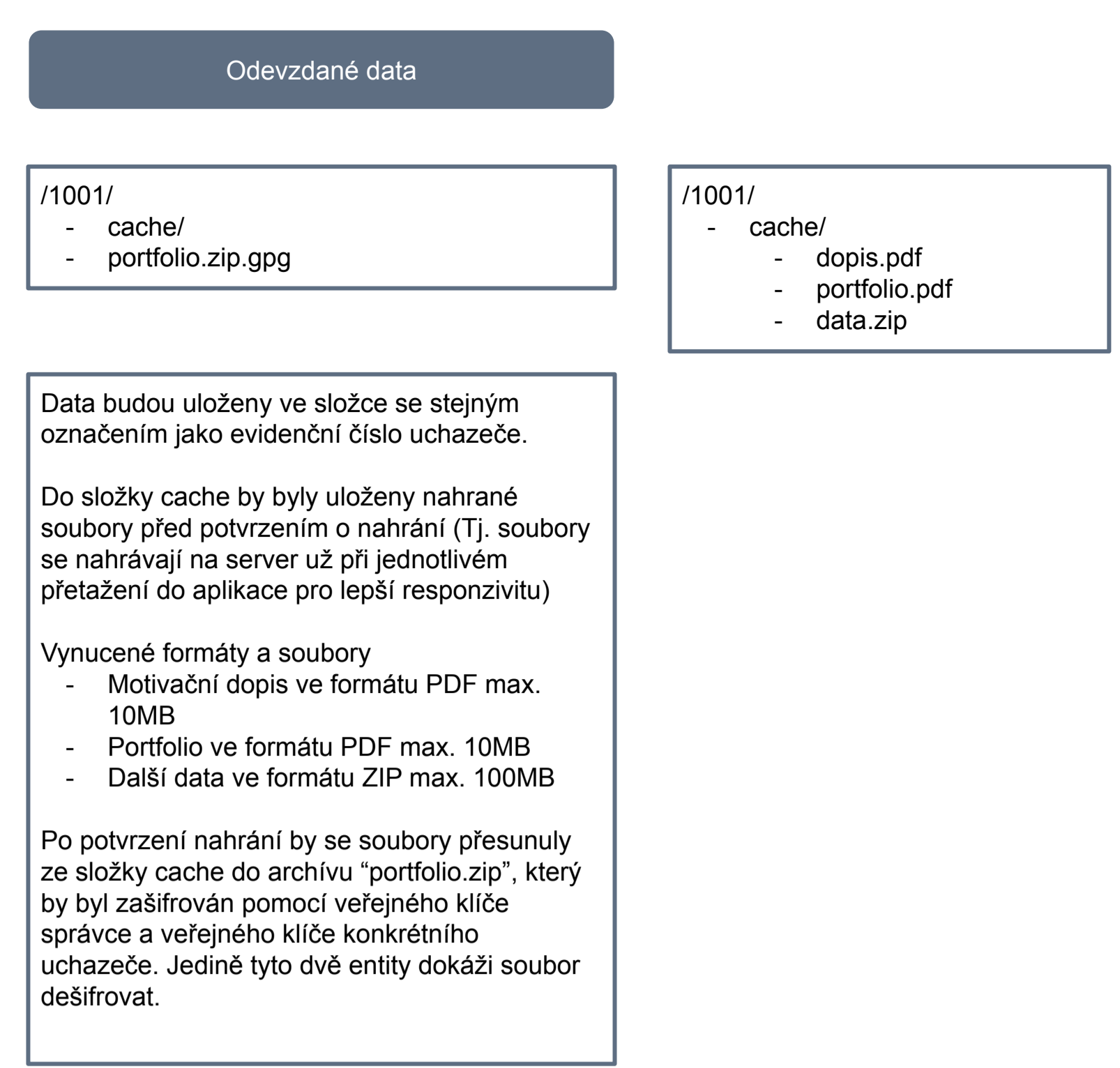
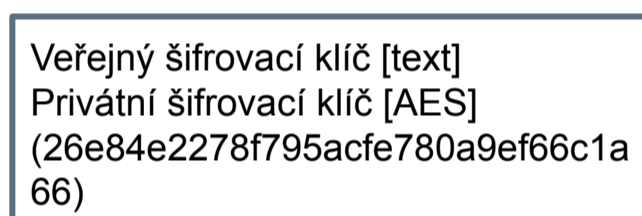
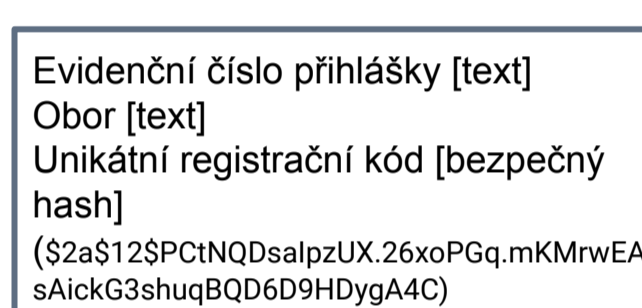
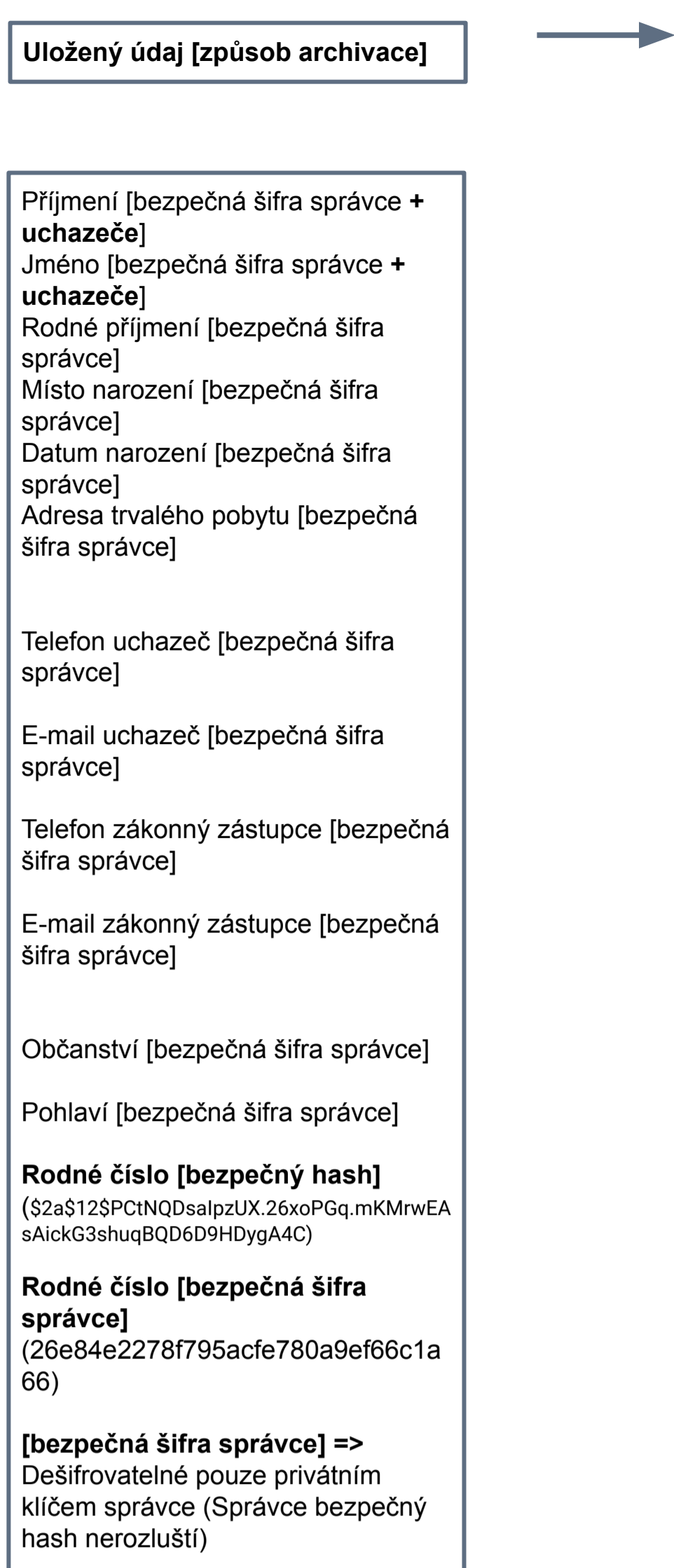
Data, včetně údajů v databázi, by byly v pravidelných intervalech zálohovány přes službu cron na jiné školní uložení. Jedná se maximálně o 170GB dat, očekávané zaplnění kapacit je spíše 50GB. V případě možného výpadku školního serveru, nebo portálu samotného, bude připravený program záchrany, který dokáže s pomocí privátního klíče správce data získat do čitelné podoby i bez součinnosti školního serveru, či portálu.

Garance jednoduchosti

Správce i uchazeč dostane jednoduché webové UI, generování přístupových kódů. Schopnosti webového rozhraní jsou popsány již v jednotlivých pravomocích obou druhů uživatelů.

Po zadání osmimístného alfanumerického kódu (Tj například. A729B17S) do přihlašovací stránky dostane uchazeč přístup do portálu s maximálním důrazem na vyplnění všech údajů z přihlášky.

V případě vyplnění všech požadovaných dat bude uchazeč přesunut a vyzván k nahrání všech jeho souborů. Potvrzení o nahrání bude dostatečně výrazně zobrazeno, naopak pakliže soubory stále chybí, bude uchazeč urgentně varován. Data bude moci kdykoli do posledního termínu pro odevzdání portfolia pozměnit.



Jak funguje šifrování veřejným a privátním klíčem?

