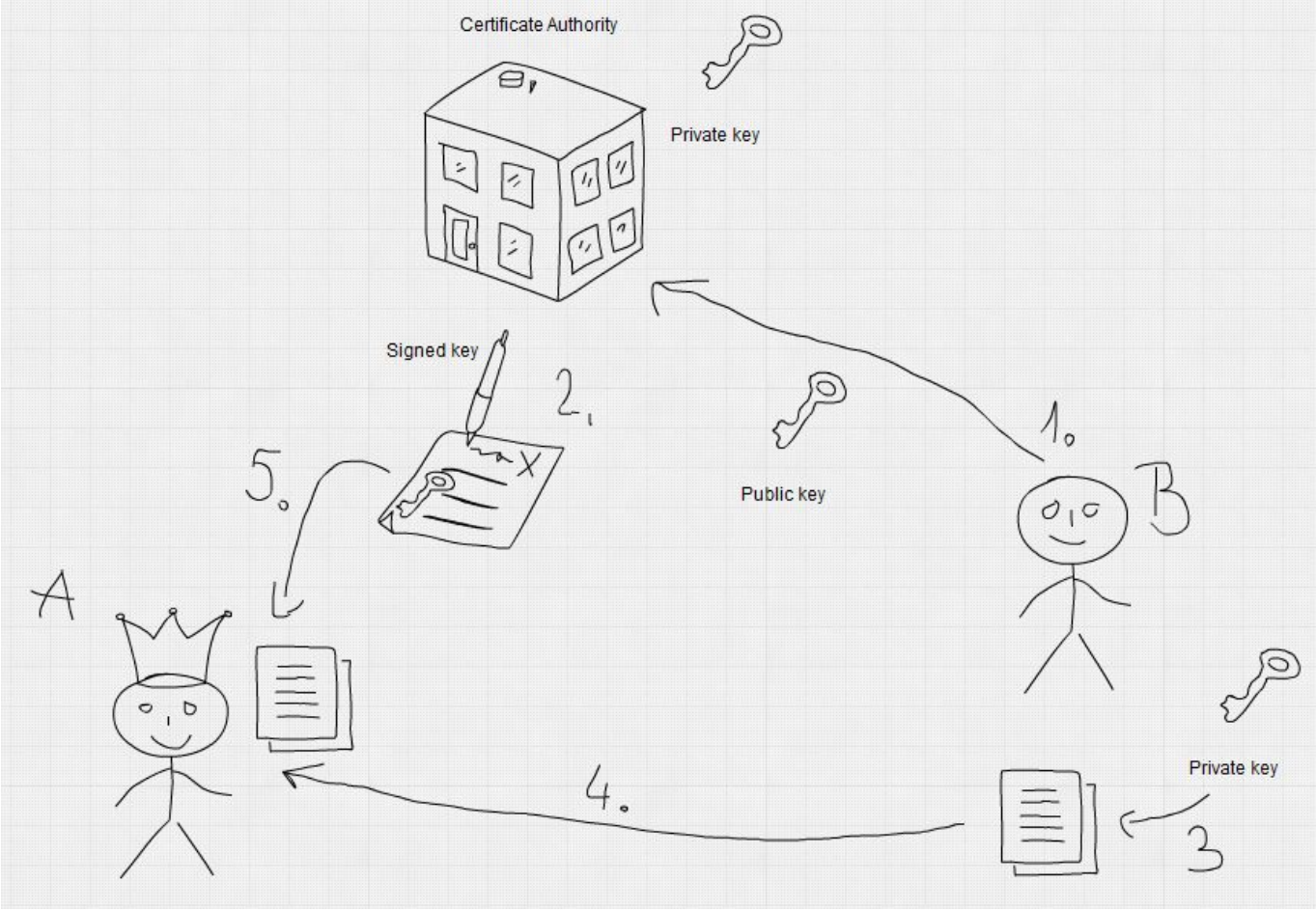
Nyilvános kulcsok hitelesítése

A legveszélyesebb helyzet akkor áll elő a kommunikációban, amikor egy rosszindulatú támadó közbeékelve a kommunikációs csatornában észrevétlenül megváltoztatja a kulcsokat. Ezt úgy lehet kivédeni, hogy egy megbízható harmadik személy segítségét kérjük aki további hitelesítést nyújt.

Milyen lépésekből áll a hitelesítés?



1. Egy tanúsítványban egy un. hitelesítő hatóság (Certificate Authority, **CA**) saját digitális aláírásával hitelesíti egy személy nyilvános kulcsát. Feltételezzük, hogy **CA**-ban mindkét kommunikáló fél megbízik.
2. Előáll egy olyan nyilvános kulcs, ami a **CA** digitális aláírását tartalmazza.
3. Berci a szokásos módon a titkos kulcsát használja (Private key) a dokumentumának titkosítására.
4. Elküldi Annának a kódolt üzenetet.
5. Ha Anna a hitelesített nyilvános kulccsal olvasni tudja az üzenetet, akkor azt biztosan Berci küldte.

Egy közbeékelt támadó nem tudja megváltoztatni a kulcsot, mert azt egy megbízható harmadik fél írta alá.

Miben kell megbízni a hitelesítő hatósággal kapcsolatban?

Abban, hogy a saját titkos kulcsa nem kerülhet nyilvánosságra.

A hitelesítés nem ingyenes. A szabványok előírják, hogy a hitelesített aláírás csak egy előre

meghatározott ideig érvényes.