Klucz prywatny (klient)
„id_dsa”

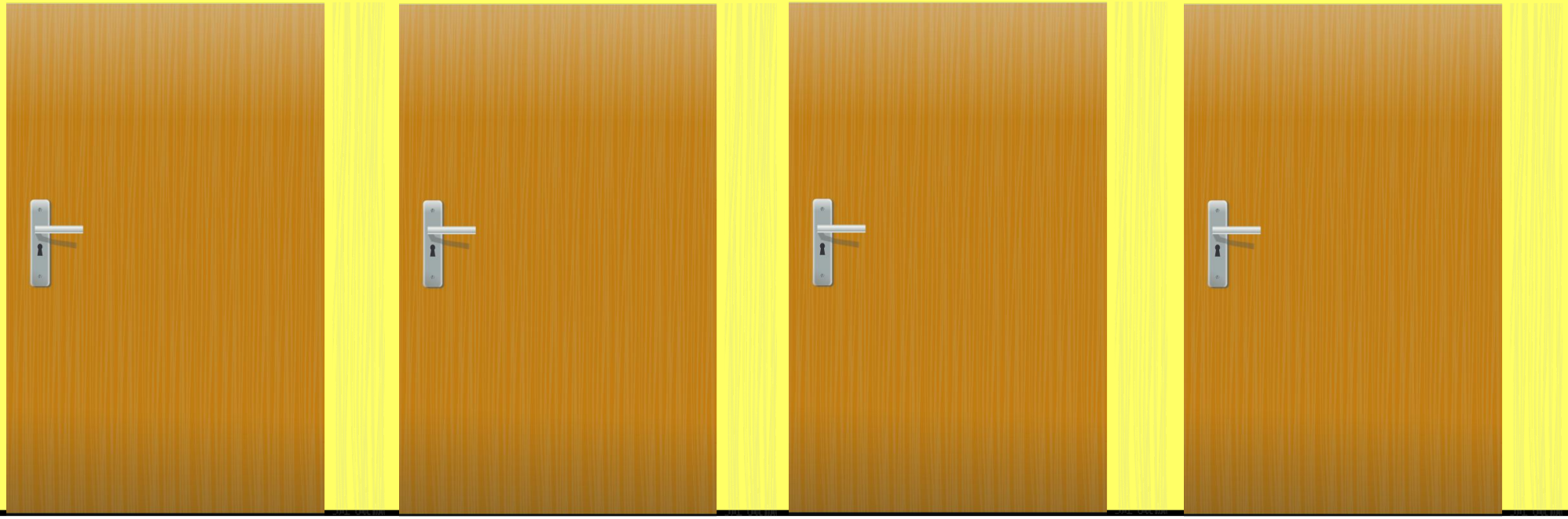
Nikomu go nie dajesz,
bo kluczy ze swojego mieszkania
także nikomu nie dajesz, prawda?

Zamek publiczny (serwer)
„id_dsa.pub”

Czyli Twoje drzwi z zamkiem, które
wstawiasz do budynku (komputera),
do którego chcesz wejść.

My system is my castle!

Do naszego domu, możemy wstawić wiele drzwi z różnymi zamkami (zamki publiczne). I choć są publiczne (bo dla każdego dostępne), to mogą otworzyć je tylko osoby mające odpowiedni klucz (klucz prywatny).



Teoria względności kluczy

Po wygenerowaniu w systemie klucza i drzwi z zamkiem, mamy dwie możliwości:

- zostawiamy w systemie **klucz prywatny** (klient) i przenosimy **drzwi** do innego systemu (serwer);

- zostawiamy **drzwi** w systemie (serwer), a przenosimy **klucz prywatny** do innego systemu (klient).

Formaty certyfikatów i kluczy

*.**cer /** *.**cert /** *.**pem** - binarny certyfikat zgodny ze specyfikacją X.509, zawiera publiczny klucz oraz informacje o właścicielu;

*.**crt** - certyfikat stworzony w openSSL;

*.**pvk** (***P****ri****V****ate* ***K****ey*) - klucz prywatny w formacie Microsoft;

*.**pfx** (*Personal Exchange Format*) - archiwum Microsoft w standardzie PKCS12 zawierające zarówno certyfikat (klucz publiczny), jak i klucz prywatny (zabezpieczony hasłem);

*.**jks** (***J****ava* ***K****ey* ***S****tore*) - certyfikat Java