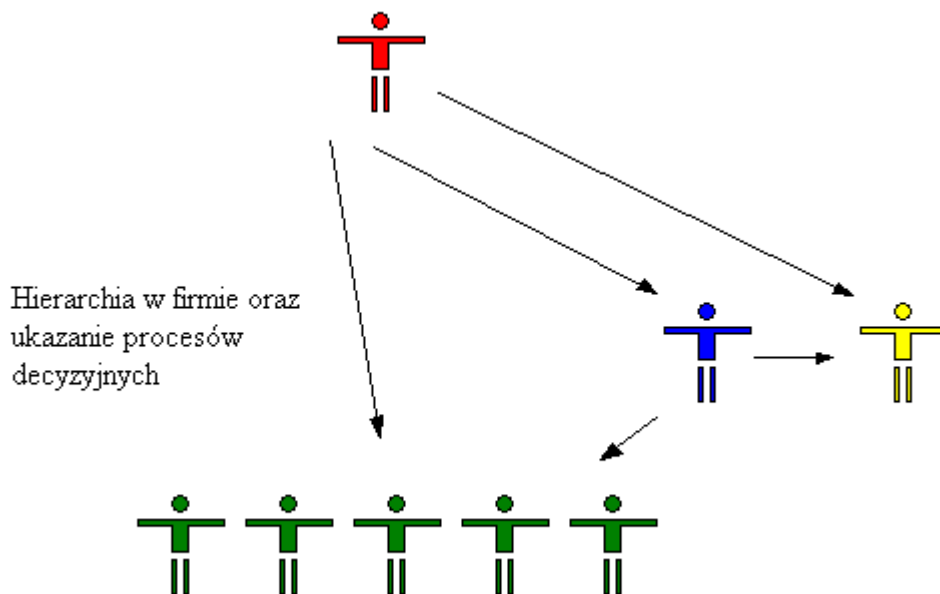
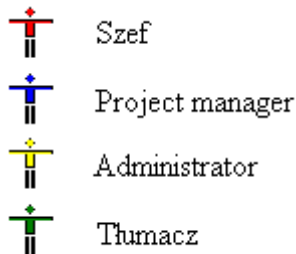
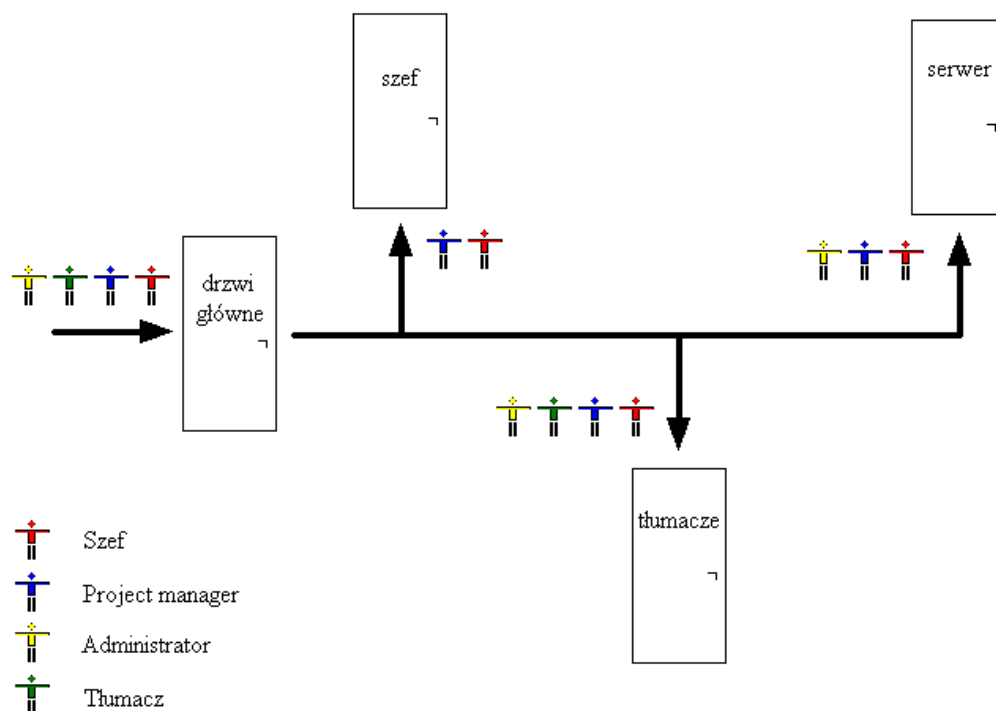


Nasza firma składa się z piętnastu pracowników. Dziesięcioro z nich wykonuje swoją pracę poza siedzibą szczecińską. Zajmujemy się lokalizacją oprogramowania komputerowego oraz instrukcji obsługi urządzeń elektronicznych.

Oznaczenia stanowisk w naszej firmie:

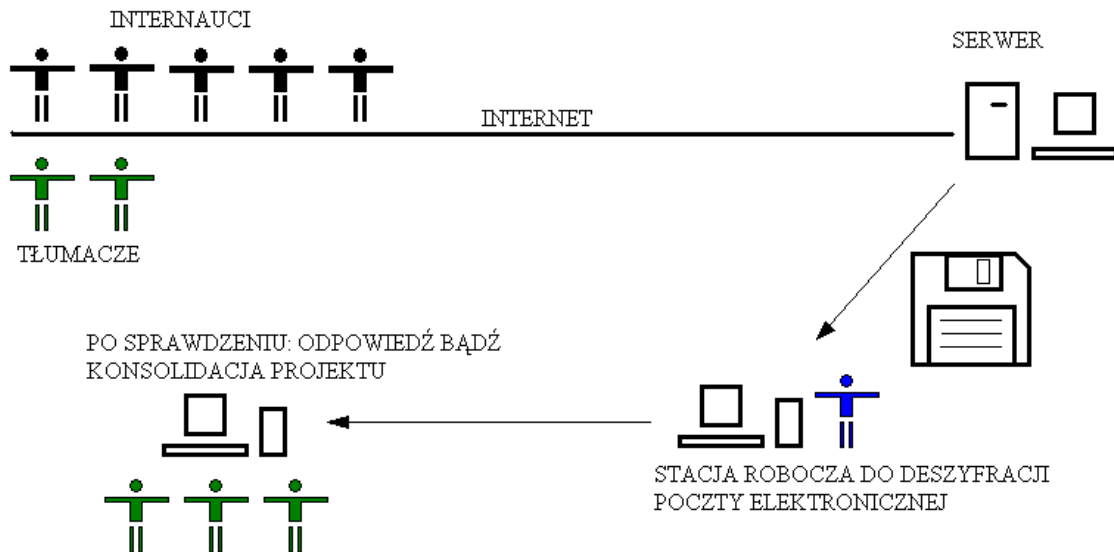


Szef wydaje zgodę *administratorowi sieci* wewnątrzfirmowej na autoryzację nowo przyjętego pracownika. Firma zatrudnia również pracowników wykonujących tłumaczenia poza siedzibą firmy. Obecnie jest pięciu tłumaczy. Każdy generuje swój klucz publiczny i prywatny za pomocą programu PGP. Klucz publiczny przesyła via e-mail do siedziby firmy, a stamtąd otrzymuje klucz publiczny *project managera*, który zarządza podziałem obowiązków między poszczególnych pracowników. Dostęp do wszystkich kluczy publicznych posiadają trzy zaufane osoby w firmie: *szef*, *project manager* oraz *administrator sieci*. Klucze prywatne pracowników szczecińskich generowane są na jednej ze stacji roboczych nie podłączonych do sieci, a znajdujących się w serwerowni, do której dostęp mają też jedynie *szef* i *project manager*. Ta stacja robocza, wraz z dokumentami i oryginalnym oprogramowaniem niezbędnym do prawidłowego działania firmy jest zamykany w kasie pancernej w serwerowni. Klucz posiada *szef* i *project manager*. Firma posiada dwa serwery: pierwszy podłączony do Internetu, drugi obsługuje pokój tłumaczy. Wszyscy pracownicy zaopatrzeni są w karty chipowe z ich ID. Bez tego żaden pracownik nie jest w stanie wejść do szczecińskiej siedziby firmy. Przy wejściu znajdują się drzwi otwierane po włożeniu do czytnika karty chipowej. W siedzibie firmy znajdują się cztery czytniki sterujące otwieraniem drzwi:



Na powyższym rysunku widać, kto posiada dostęp do poszczególnych pomieszczeń. Petenci nie są przyjmowani. Nawet, jeśli osoba trzecia dostanie się na korytarz główny, nie będzie ona mogła przedostać się do kluczowych pomieszczeń. Co najwyżej będzie miała dostęp do ubikacji i pokoju wypoczynkowego dla pracowników.

Zlecenia z głównej siedziby firmy przyjmowane są głównie za pośrednictwem Internetu. Klucz publiczny głównej siedziby oraz wszystkich filii, przechowywany jest w stacji roboczej w serwerowni. Klucze publiczne nie są rozdawane osobom trzecim tak, jak i nie są dostępne na stronie internetowej firmy. Dotyczy to klucza publicznego „do kontaktów wewnętrznych” firmy. Na stronie internetowej natomiast udostępniony jest klucz publiczny filii „do kontaktów zewnętrznych” oraz „odcisk palca”. Każdy człowiek chcący przesłać zaszyfrowane informacje dla firmy, może ściągnąć nasz klucz „do kontaktów zewnętrznych” i za jego pośrednictwem przesłać dane. Po ściągnięciu całej korespondencji na serwer, jest ona przegrywana na dyskietkę i przenoszona przez administratora do project managera, który na stacji roboczej nie podłączonej do sieci, wykonuje proces deszyfracji, sprawdzenia oprogramowaniem antywirusowym i odczytania danych. Jest to zabezpieczenie na wypadek umieszczenia w korespondencji wirusów, gdyż każdy może nam wysłać wrogiego bakcyła. W przypadku uaktywnienia wirusa, zostanie zainfekowana jedynie jedna stacja robocza.

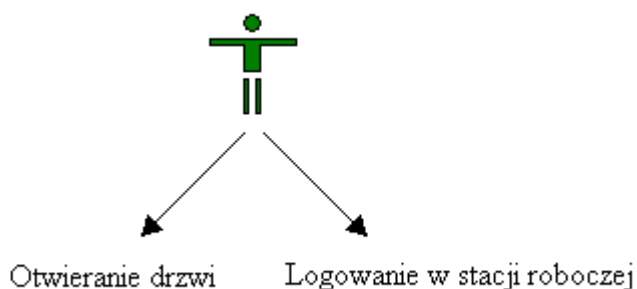
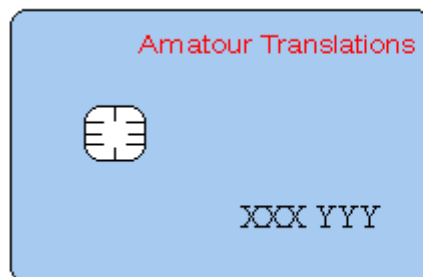


Każdy z pracowników jest zobowiązany po rozwiązaniu umowy o pracę, zwrócić kartę chipową *project managerowi*. Pracownicy zatrudnieni na okres próbny trwający 5 dni, nie posiadają karty. Są wpuszczani do siedziby przez *project managera* od godziny 8:00 do 8:15 każdego dnia roboczego. Karty są ważne 1 rok. Wymieniane są 1 lipca każdego roku. Jeżeli pracownik jest przyjęty po tym dniu, ma generowany klucz, wyrabianą kartę, lecz ważną tylko do 1 lipca nawet, gdyby został zatrudniony w czerwcu. Jest to wprowadzone ze względu na wygodę. Używane są klucze kodowe o długości 4096 bitów. Złamanie kodu jest niemożliwe w tak krótkim okresie czasu jak rok (przy obecnym zaawansowaniu technologicznym).

Zadania przydzielane pracownikom znajdującym się poza siedzibą firmy (w innym mieście) są wydawane przez *project managera*. Każdy mail jest szyfrowany oraz dodatkowo podpisywany cyfrowo przez niego. Zwrotna poczta od pracownika nie wymaga stosowania podpisu cyfrowego, najważniejsze jest, by pakiet otrzymany został poprawnie przetłumaczony. Przepływ informacji typu: numer konta, na które dokonywać przelewu poborów, również wykonuje się za pośrednictwem tej samej drogi, jak poprzednio. Nie korzystamy z rozwiązań tradycyjnych, jak poczta i telefon, gdyż poziom zabezpieczeń jest zerowy.

Pracownik XXXX YYY

Karta zawiera:
Imię i nazwisko
PESEL
Poziom dostęp
Klucz publiczny i prywatny PGP



Każdy z tłumaczy posiada swoją stację roboczą nie podłączoną do Internetu, a jedynie spiętą w małą sieć wewnątrz pokoju tłumaczy. Ma to zapobiec atakom „końmi trojańskimi” oraz trwonieniu czasu przez pracowników. Sieć jest niezbędna, by przepływ informacji między stacjami roboczymi był duży. Dostęp do Internetu posiadają: *szef, project manager, administrator sieci*. Każda ze stacji roboczych zaopatrzona jest w najtańszy czytnik kart chipowych, umożliwiających identyfikację pracownika. Zapobiega to dostępowi tłumaczy nawzajem do swoich tłumaczeń. Ma to na celu uniknięcie pomyłek, robieniu głupich żartów oraz „podkładaniu świń” przez pracowników. Bierzemy pod uwagę, iż ludzie mogą być do siebie negatywnie nastawieni.