FCR

Fast Certified Reliable

Zdrowie w chmurze

Tadeusz Reczyński
Stefan Sterzycki
FCR sp. z o.o.

CommonSign Warszawa 2016

Fast Certified Reliable

AGENDA PREZENTACJI

- Dlaczego znowu o chmurze – ogólne wprowadzenie
- Bezpieczna – zdrowa chmura: tak czy nie?
- Nieco inne podejście do problematyki bezpieczeństwa w chmurze
- Przykładowe wykorzystanie

Fast Certified Reliable

O czym warto porozmawiać

- Cel i sens wykorzystania podpisu elektronicznego:
  - wymiana informacji,
  - skuteczne, także w sensie prawnym, wykonywanie czynności –
  - niezależnie od miejsca i czasu
- A to oznacza przeniesienie się w przestrzeń abstrakcyjną - chmurę:
  - gdzieś, lecz często nie wiadomo gdzie,
  - gdzie ktoś ważniejszy, posiadający większe możliwości, większą wiedzę (a wiedza oznacza władzę),
  - przejmuje kontrolę nad ważnymi dla właściciela obiektami,
- Mimochodem, niezauważalnie, pojawiła się nowa *religia*, z nieodłącznym atrybutem niepewnej *przyszłości cyfrowej* oraz *guru* w wielu osobach:
  - Nie możesz ... – skontaktuj się z ...
  - Zapomniałeś ... – skontaktuj się z ...
  - ON – omnipotentny Administrator Twojej Chmury!

Fast Certified Reliable

O czym warto porozmawiać – bez ironii

- Z różnych kanałów docierają, oczekiwane, ale częściej niechciane, oferty zawierające gwarancję bezpieczeństwa w chmurze,
- Potencjalnie – deklaruje je każdy administrator,
- Zazwyczaj deklaracje są szczere
  - kryją się za nimi poważne inwestycje,
  - odpowiada za nie wyspecjalizowany personel,
  - są opatrzone certyfikatami,
  - zawierają stosowną politykę bezpieczeństwa
- Nie mniej...

Fast Certified Reliable

O czym warto porozmawiać – bez ironii

- Coraz częściej docierają do opinii publicznej liczne informacje o zaskakujących czy wręcz niewiarygodnych włamaniach do zasobów instytucji, które trudno podejrzewać o beztroskie traktowanie zagadnień bezpieczeństwa,
- Po ujawnieniu włamania ogłaszane są przyczyny:
  - beztroska użytkowników,
  - nonszalancja,
  - nieprzestrzeganie procedur,
  - niski poziom świadomości.
- Krótko – winni są ludzie
  - tyle, że to nie zła wola,
  - to natura człowieka

FCR

Fast Certified Reliable

Natura człowieka

- rozwiązanie login/hasło jest niewygodne a zatem podatne na *optymalizację* ze strony użytkowników:
  - zapisywanie haseł,
  - stosowanie tych samych par login/hasło w wielu aplikacjach,
  - niechęć do zmieniania haseł.
  - ...
- większość udanych ataków pochodzi z wewnątrz organizacji,
- administratorzy i personel serwisowy systemów IT mają mniej lub bardziej swobodny dostęp do zasobów informacyjnych, np. danych biznesowych,
- a z naturą walka daremna – podstawowa zasada inżynierska: *prawami przyrody nie należy walczyć – nie ma szans na ich pokonanie; do praw natury należy się stosować.*

Nieco inne podejście

Fast Certified Reliable

- Security by Design – system projektowany od warstwy bezpieczeństwa

Security by design

Fast Certified Reliable

- Wykorzystanie znanych a zarazem nowoczesnych rozwiązań technicznych:
  - standardu XML,
  - kwalifikowanego podpisu elektronicznego,
  - tworzenie dokumentu w formacie XML Advanced Electronic Signature (XAdES),
- Włączenie procesu w obieg istniejącej infrastruktury:
  - Internet,
  - dostęp poprzez przeglądarki internetowe,
  - możliwość integracji z wewnętrznym procesem workflow instytucji
  - Wykorzystanie instytucja zaufania publicznego,

FCR

Fast Certified Reliable

Security by design

- Rozdzielenie funkcji technicznych i merytorycznych
  - Wykluczenie możliwości uzyskania dostępu do przetwarzanej informacji przez osoby nieuprawnione,
  - niezależnie od ich uprawnień związanych np. z administrowaniem infrastrukturą teleinformatyczną lub jej serwisowaniem.
- Mocne szyfrowanie danych
  - Transmitowanych
  - Przechowywanych
- Dwuaspektowe uwierzytelnianie
  - Oparte o algorytmy niesymetryczne
  - Klucze prywatne na kartach kryptograficznych, lub w postaci zaszyfrowanej w trudno dostępnych zasobach stacji roboczej,

Security by design

Fast Certified Reliable

- przypisanie do każdego przechowywanego atrybutu list zarządzania dostępem (*ang*. Access Control List) oddzielnych dla każdego trybu dostępu: tylko przeglądanie, przeglądanie i modyfikacja etc. – elementami tych list mogą być pojedyncze osoby lub całe zespoły;
- możliwość blokowania kopiowania lub drukowania;
- prowadzenie dla każdego dokumentu szczegółowego dziennika dostępów;
- możliwość opatrzenia dokumentu klauzulą poufności, blokującą dostęp do treści dokumentu osobom bez odpowiedniego poziomu dopuszczenia, nawet jeśli mają dostęp do jego opisu i innych metadanych.

Wydajność i dostępność

- Wymóg wydajności oznacza konieczność projektowania z dogłębną znajomością rzeczy, w tym starannego zaplanowania struktur danych i mechanizmów wyszukiwania.
- Dostępność – skalowalna zabezpieczona platforma systemowa
  - High availability
    - Redundancja systemu i jego konfiguracji
    - Wiele dróg dostępu do internetu
  - Backup / recovery
  - Ochrona przed DDoS itp.

FCR

Fast Certified Reliable

Repozytorium

- Wbudowane bezpieczeństwo
- Rozliczalność
  - Każde zdarzenie jest rejestrowane
    - Dwupoziomowa historia zmian
  - Odseparowanie administracji od biznesu
  - Niezawodność
- Dokładny opis i precyzyjne wybieranie
  - Konfigurowalne metadane
  - Adnotacje
  - Łatwość konfigurowania własnego pulpitu dostępu
- Konfigurowanie zadań
- Powiadamianie kontekstowe – zadaniowe.

FCR

Fast Certified Reliable

Repozytorium / dokumenty

- Meta-opis dokumentów / artefaktów
  - Dogodne komentowanie zawartości (z różnymi prawami dostępu)
  - Wybieranie / filtrowanie
- Kontekstowe zarządzanie prawami dostępu
- Stosowanie polityki klauzul poufności (KNF)
- Szyfrowanie zawartości
- Powiadomienia o zmianach
- Automatyczne wersjonowanie zmian w plikach
  - Podgląd wszystkich wersji
    - Historia wszystkich zmian
  - Ale także faktu wyświetlenia dokumentu!
- Wbudowane podpisywanie XAdES

Integracja

Fast Certified Reliable

- Platforma SiC ma wbudowane duże możliwości integracji
  - Interfejs programistyczny (API) umożliwia dodawanie nowych funkcji i integrowanie z innymi systemami bez współpracy dostawcą
- Platforma SiC obsługuje dodatkowe funkcje
  - Dwustronna skrzynka podawcza
  - Moduł kancelaryjny
  - Konfigurowany CRM
  - bezpieczna wymiana korespondencji

FCR

Fast Certified Reliable

Przykładowe zastosowanie:

Historia pewnego orzeczenia

Przykład metody ułatwiania obiegu wrażliwych dokumentów medycznych

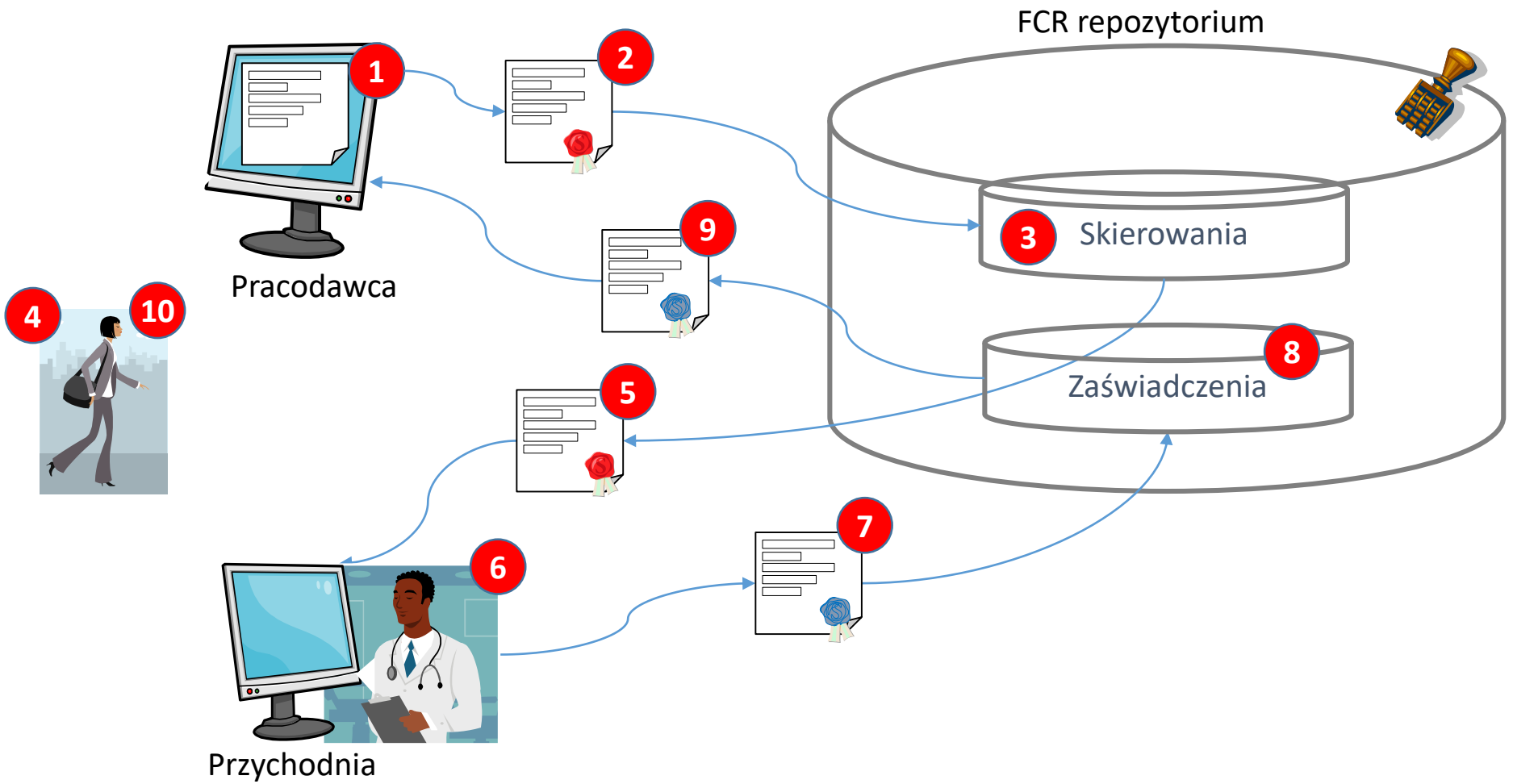
E-orzeczenie

procedury Służby Medycyny Pracy

- system powszechny,
- obejmuje wszystkich aktywnych zawodowo,
- korzystających z systemu wielokrotnie,
- generuje często bardzo obszerne informacje o stanie zdrowia pacjenta,
- przemieszczane na wskroś przestrzeni publicznej,
- w systemie działającym od lat, zorganizowanym w sposób tradycyjny, dane te nie są właściwie chronione.

Proces obsługi E-orzeczenia

Fast Certified Reliable



Fast Certified Reliable

E- orzeczenie a platforma SiC

- Radykalne ograniczenie ryzyka ujawnienia danych wrażliwych,
- Zmniejszenie kosztów procesu, w tym:
  - kosztu przerwy w pracy spowodowanej nie dostarczeniem na czas ważnego zaświadczenia o zdolności do wykonywania pracy,
  - kosztów sporu pomiędzy wykonawcą usługi a pracodawcą (?)
- Szybszy i pewny proces wymiany dokumentów,
- Ułatwienie realizacji procedur formalnych

FCR

Fast Certified Reliable

Dziękuję

Tadeusz Reczyński

FCR Sp. z o.o.

Tadeusz.Reczynski@fcr.net.pl