Podpis Administracyjny (PA)

koncepcja projektu EZD RP

Założenia

Poniższe założenia stosują się do obu wariantów. Komponenty techniczne, niezbędne do korzystania z PA będą zlokalizowane zarówno w warstwie centralnej (UCPA), jak lokalnej (ULPA), w podmiocie publicznym.

CCPP

Minister właściwy ds. informatyzacji wyznaczy podmiot, który będzie odpowiedzialny za wystawianie certyfikatów (Centrum Certyfikacji Podmiotów Publicznych – CCPP) dla podmiotów realizujących zadania publiczne, czyli objętych art.13a ustawy o informatyzacji podmiotów realizujących zadanie publiczne. CCPP będzie – w ścisłej współpracy z Katalogami Administracji Publicznej (KAP) – udostępniało podmiotom publicznym certyfikaty, umożliwiające jednoznaczną identyfikację tych podmiotów. Zarówno utworzenie certyfikatu, jak jego użycie, możliwe będzie jedynie za pośrednictwem systemu teleinformatycznego podmiotu publicznego, dysponującego certyfikatem wystawionym przez CCPP.

UCPA

Minister właściwy ds. informatyzacji wyznaczy podmioty, które będą odpowiedzialne za wystawianie certyfikatów imiennych dla pracowników podmiotów publicznych, świadcząc Usługi Centralne Podpisu Administracyjnego (UCPA). Podmiot prowadzący UCPA uzyska pieczęć niezbędną do wystawiania certyfikatów koniecznych do składania PA, której certyfikat opatrzony będzie pieczęcią ministra właściwego ds. informatyzacji („root"). W UCPA przechowywana będzie informacja o powiązaniu numeru PESEL pracownika z identyfikatorem podmiotu publicznego i unikatowym identyfikatorem pracownika w tym podmiocie

ULPA

Podmioty publiczne, dysponujące certyfikatem CCPP, dysponować będą oprogramowaniem ULPA (Usługi Lokalne Podpisu Administracyjnego) zapewniając poprawność i aktualność przetwarzanych w ULPA danych w zakresie stanowiska pracownika, jego imienia, nazwiska i nr PESEL oraz jego unikatowego, w ramach podmiotu publicznego, identyfikatora. Ze względu na przewidywaną skalę wykorzystania (kilkaset tysięcy pracowników w kilkudziesięciu tysiącach podmiotów) i różnorodność lokalnych systemów teleinformatycznych podmiotów publicznych, zakłada się zróżnicowane bezpieczeństwo tych systemów, mimo istnienia wymogów określonych przepisami wydanymi na podstawie art. 18 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne.

Ergonomia

Utworzenie certyfikatu, niezbędnego do składania PA, wymaga uwierzytelnienia pracownika podmiotu publicznego z wykorzystaniem środka identyfikacji elektronicznej wydanego w systemie identyfikacji elektronicznej przyłączonym do Węzła Krajowego, a złożenie PA wymaga jedynie podania hasła ustalanego przez użytkownika, przy czym nie będzie się wymagać hasła dłuższego, niż 8 znaków alfanumerycznych. Zablokowanie możliwości składania PA realizowane będzie na żądanie pracownika (po uwierzytelnieniu przez Węzeł Krajowy) lub na żądanie upoważnionego przedstawiciela podmiotu publicznego.

Bezpieczeństwo

Wszystkie komponenty PA zbudować należy z modułów zgodnych ze standardami PKI, przy wykorzystaniu standardowych protokołów i „ścieżki certyfikacji" oraz zachować pełną zgodność z normami PKI. PA nie umożliwi poznania numeru PESEL podpisującego, a jedynie jego imienia, nazwiska, stanowiska oraz identyfikatora. Do ustalenia numeru PESEL podpisującego niezbędne będzie odwołanie do dedykowanej, niedostępnej powszechnie, usługi UCPA.

Zostaną zapewnione narzędzia umożliwiające rozliczalność użycia podpisu.

Wydajność

Wymagana wydajność serwisu powinna docelowo pozwalać na składanie co najmniej 10^9 PA rocznie z założeniem, że zdecydowana większość tych podpisów składana będzie w dni powszednie, w godz. 8^{00}-16^{00};

Prawo

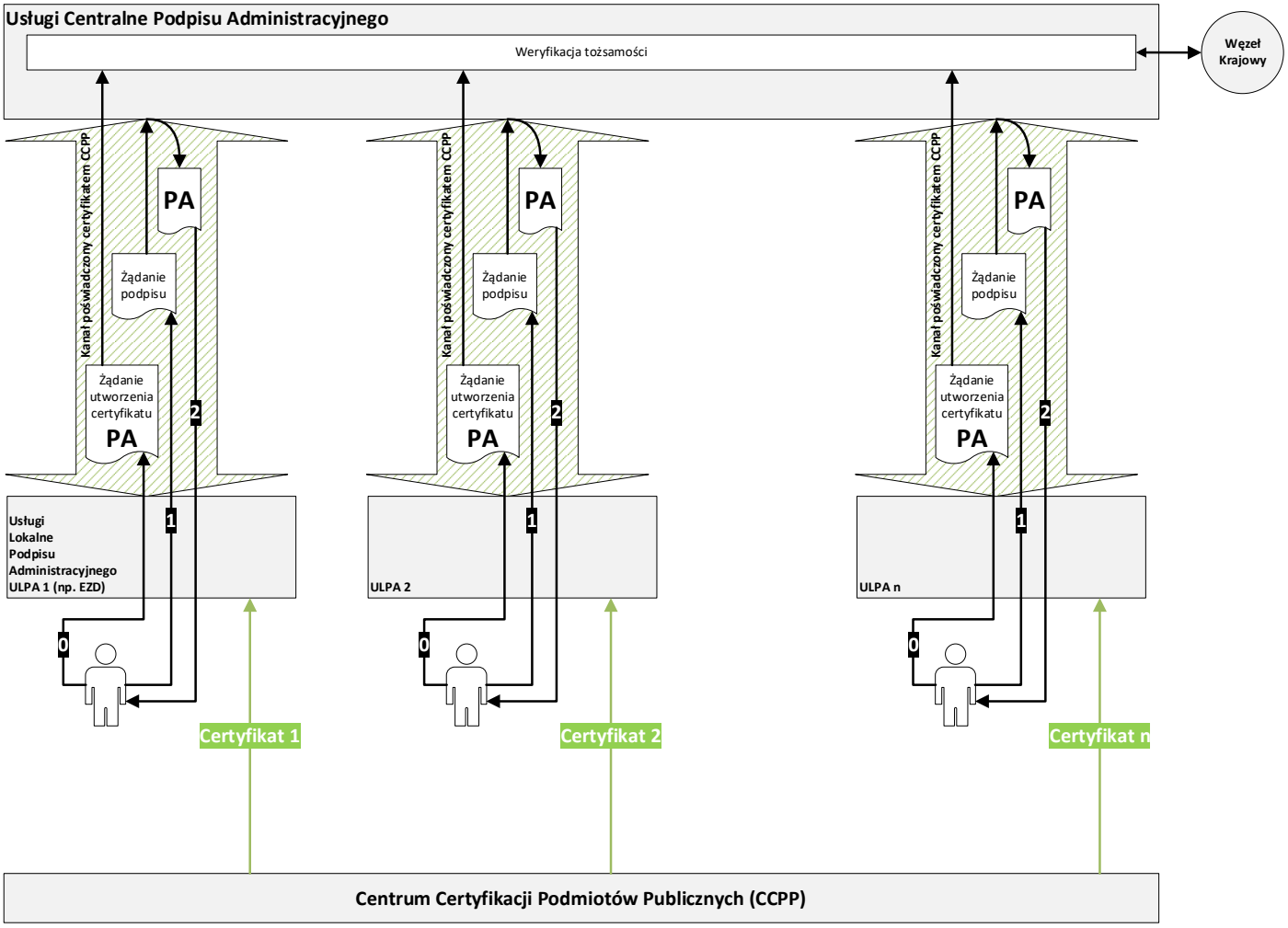
PA będzie umocowany prawnie jako wariant Podpisu Zaufanego z tym, że jego użycie będzie dopuszczalne wyłącznie, gdy podpisujący działa w imieniu podmiotu publicznego w rozumieniu w art. 2 i art. 19c ust. 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (A2A, A2B i A2C), a wyłączona zostanie możliwość podpisywania PA innych dokumentów (C2C, C2B, B2B, B2C).

Proces uzyskiwania i składania podpisu (taki sam w obu wariantach)

Opis.

1. Zarówno uzyskanie możliwości składania PA (utworzenie certyfikatu), jak i jego używanie będzie możliwe wyłącznie w środowisku teleinformatycznym podmiotu publicznego, dysponującego certyfikatem CCPP.
2. Podpis administracyjny będzie dostępny dla pracownika podmiotu publicznego po uzyskaniu go w następujący sposób:
    a) Pracownik loguje się do systemu administracji publicznej, np. EZD;
    b) Pracownik wywołuje funkcję umożliwiającą wysłanie żądania wystawienia certyfikatu podpisu, w ramach którego podawane są dane: imię, nazwisko, stanowisko, PESEL, identyfikator pracownika;
    c) System, w którym są wydawane certyfikaty, przyjmuje żądanie i wysyła do pracownika prośbę o potwierdzenie tożsamości, czyli pracownikowi prezentowana jest strona login.gov.pl;
    d) Potwierdzenie tożsamości odbywa się poprzez dwuskładnikowe uwierzytelnienie za pośrednictwem WK;
    e) Dopuszczalne jest uwierzytelnienie wszystkimi środkami dostępnymi na WK (zarówno środkami publicznymi, jak i komercyjnymi);
    f) Po potwierdzeniu zgodności danych (imię, nazwisko, numer PESEL z żądania = imię, nazwisko, numer PESEL z środka identyfikacji) generowany jest standardowy certyfikat zaawansowanego podpisu elektronicznego dla którego pracownik ustanawia hasło (np. PIN znany tylko pracownikowi). Klucz prywatny jest zaszyfrowany hasłem określonym przez pracownika;
    Certyfikat podpisu zawiera imię, nazwisko i unikatowy identyfikator certyfikatu wygenerowany przez podmiot wydający certyfikat, dane podmiotu, który reprezentuje osoba dla której wystawiono certyfikat oraz stanowisko pracownika.;
    g) Możliwość unieważnienia certyfikatu ma podmiot publiczny, na żądanie którego certyfikat został wygenerowany oraz pracownik dla którego certyfikat został wydany.
    h) Podmiot publiczny w swoim systemie posiada narzędzia umożliwiające rozliczalność użycia podpisu.
3. Użycie podpisu
    a) W celu wykorzystania podpisu należy zalogować się w systemie np. EZD;
    b) Nie jest wymagane każdorazowe uwierzytelnienie login.gov.pl;
    c) Użycie podpisu wymaga jedynie podania hasła ustanowionego przez pracownika.

Schemat.


Usługi Centralne Podpisu Administracyjnego
Weryfikacja tożsamości
Węzeł Krajowy
Kanał poświadczony certyfikatem CCPP
PA
Żądanie podpisu
Żądanie utworzenia certyfikatu
PA
2
1
0
Usługi Lokalne Podpisu Administracyjnego ULPA 1 (np. EZD)
ULPA 2
ULPA n
Certyfikat 1
Certyfikat 2
Certyfikat n
Centrum Certyfikacji Podmiotów Publicznych (CCPP)

Wariant I – realizacja centralna

PA będzie (technicznie) standardowym zaawansowanym podpisem elektronicznym, weryfikowanym za pomocą niekwalifikowanego certyfikatu, generowanym centralnie przez UCPA, po podaniu kodu PIN określonego wcześniej przez podpisującego. Klucz prywatny przechowywany będzie w audytowanym i certyfikowanym środowisku UCPA. PA weryfikowany będzie standardowym, dziesięcioletnim[1], opatrzonym pieczęcią UCPA certyfikatem, zawierającym imię i nazwisko użytkownika, unikatowy identyfikator podmiotu publicznego oraz unikatowy (w ramach podmiotu publicznego) identyfikator pracownika i jego stanowisko służbowe. Deklarowana data złożenia podpisu będzie ustalana przez UCPA, w związku z czym zbędne będzie opatrywanie podpisu znacznikiem czasu.

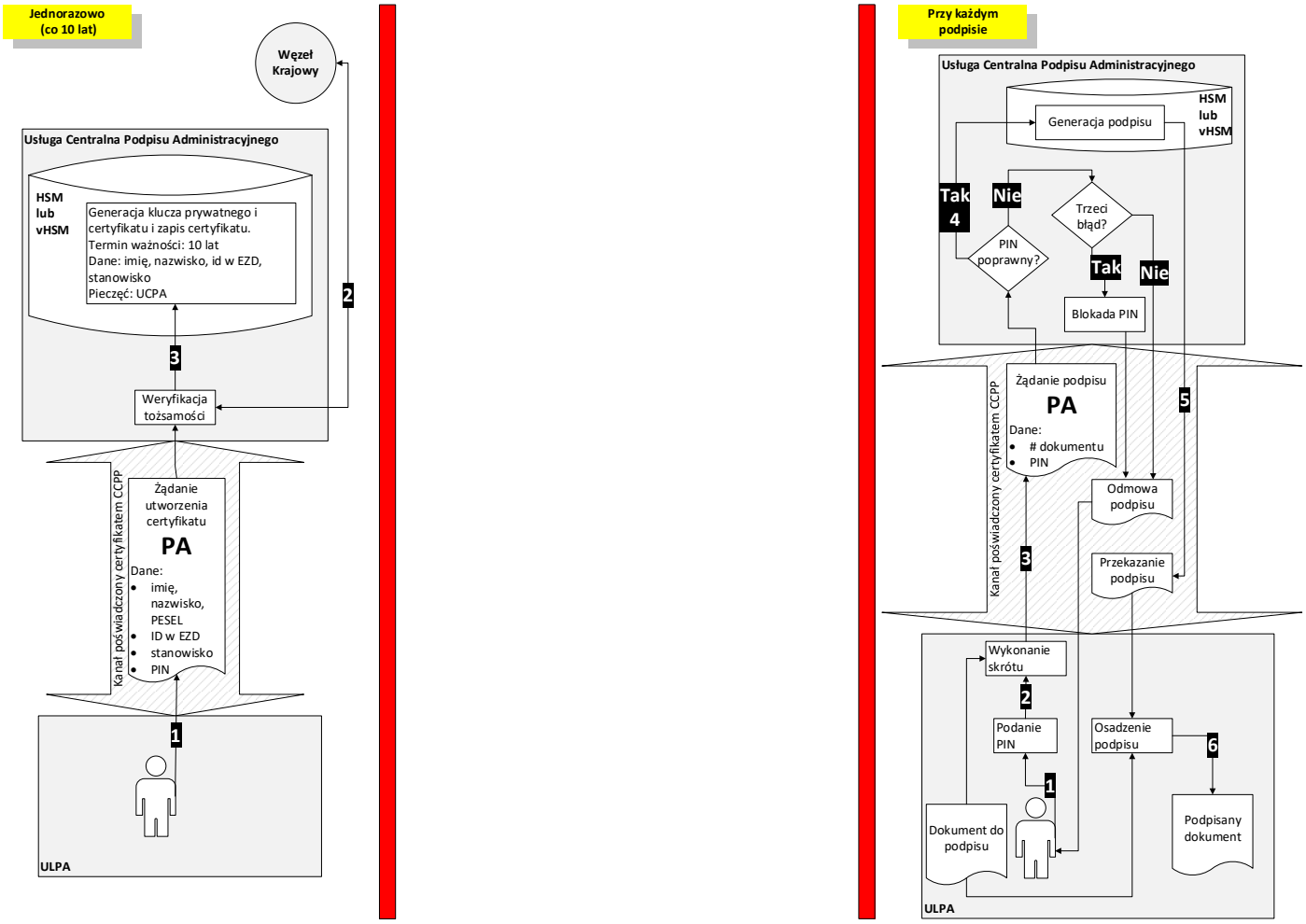
Pracownik podmiotu publicznego, chcąc korzystać z PA, będzie musiał skierować do UCPA żądanie generacji certyfikatu do podpisu PA. Żądanie musi być poświadczone certyfikatem podmiotu publicznego, wystawionym przez CCPP i – poza danymi pracownika (imię, nazwisko, PESEL) – musi zawierać unikatowy, w ramach podmiotu publicznego, identyfikator pracownika. Obsługując żądanie, UCPA weryfikuje tożsamość pracownika poprzez Węzeł Krajowy, a następnie generuje klucz prywatny i standardowy certyfikat PA.

Przy podpisywaniu dokumentu, pracownik podmiotu publicznego musi podać hasło („PIN alfanumeryczny"). ULPA wygeneruje skrót dokumentu i – wraz z hasłem – prześle do UCPA, która zweryfikuje hasło, ustali deklarowany czas podpisu jako czas bieżący i wykona podpis, używając klucza prywatnego chronionego przez audytowane i certyfikowane środowisko UCPA. Przesłany zwrotnie do ULPA podpis zostanie osadzony w dokumencie (lub – jako podpis zewnętrzny – zapisany), kończąc procedurę.

Jeśli do UCPA skierowane zostaną trzy kolejne żądania podpisu z błędnym hasłem, to możliwość wykonania PA przez danego pracownika zostanie zablokowana, a odblokowanie wymagać będzie użycia środka identyfikacji elektronicznej w Węźle Krajowym. Podobna procedura będzie wymagana dla zmiany hasła.

[1] Tak długi okres ważności certyfikatu pozwoli odsunąć problemy z konserwacją podpisu, a jest dopuszczalny, gdyż procedura składania podpisu wyklucza możliwość złożenia podpisu po unieważnieniu certyfikatu.

Schemat – wariant I



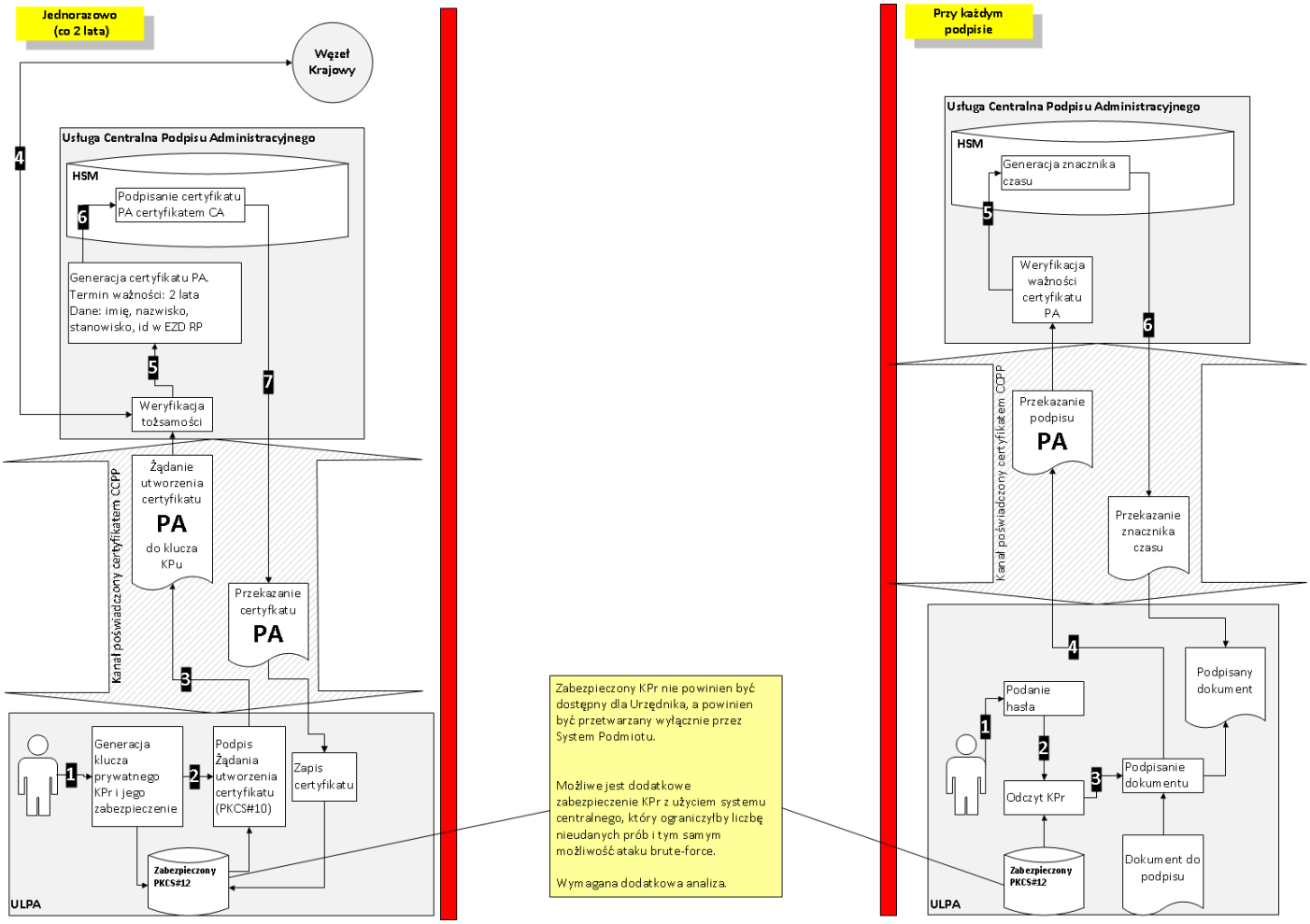
Wariant II – realizacja rozproszona

Podobnie jak w wariancie I PA będzie (technicznie) standardowym zaawansowanym podpisem elektronicznym, weryfikowanym za pomocą niekwalifikowanego certyfikatu. W przeciwieństwie do wariantu I podpis będzie generowany lokalnie przez ULPA, po podaniu kodu PIN określonego wcześniej przez podpisującego. Klucz prywatny przechowywany będzie w ULPA. PA weryfikowany będzie standardowym, ważnym dwa lata certyfikatem opatrzonym pieczęcią UCPA, zawierającym imię i nazwisko użytkownika, unikatowy identyfikator podmiotu publicznego oraz unikatowy (w ramach podmiotu publicznego) identyfikator pracownika i jego stanowisko służbowe. Każdy podpis będzie opatrywany znacznikiem czasu generowanym w HSM UCPA.

Podobnie jak w wariancie I pracownik podmiotu publicznego, chcąc korzystać z PA, będzie musiał skierować do UCPA żądanie generacji certyfikatu do podpisu PA. Żądanie musi być poświadczone certyfikatem podmiotu publicznego, wystawionym przez CCPP i – poza danymi pracownika (imię, nazwisko, PESEL) – musi zawierać unikatowy, w ramach podmiotu publicznego, identyfikator pracownika. Obsługując żądanie, UCPA weryfikuje tożsamość pracownika poprzez Węzeł Krajowy, a następnie generuje klucz prywatny i standardowy certyfikat PA. W przeciwieństwie do wariantu I klucz i certyfikat nie będą przechowywane centralnie, tylko lokalnie w systemie podmiotu publicznego. Klucz prywatny zapisany lokalnie w ULPA będzie dostępny dla urzędnika tylko wtedy, gdy będzie pracował w kontekście sytemu podmiotu publicznego.

Przy podpisywaniu dokumentu, pracownik podmiotu publicznego musi podać hasło („PIN alfanumeryczny"). ULPA wygeneruje podpis i prześle do UCPA, która zweryfikuje ważność certyfikatu i opatrzy podpis znacznikiem czasu i odeśle o ULPA kończąc procedurę.

Schemat – wariant II



Różnice pomiędzy wariantami

1. Miejsce przechowywanie danych do składania podpisu
   a) W wariancie I (centralnym) dane do składania podpisu przechowywane są centralnie w audytowanym i certyfikowanym środowisku UCPA
   b) W wariancie II (rozproszonym) dane do składania podpisu przechowywane są lokalnie w systemie podmiotu publicznego w ULPA
2. Podpis
   a) W wariancie I (centralnym) do UCPA będzie przesyłany skrót do podpisania a odsyłany będzie podpis
   b) W wariancie II (rozproszonym) do UCPA będzie przesyłany podpis a odsyłany będzie podpis opatrzony znacznikiem czasu