

Rozdział 4

Tożsamość cyfrowa EBSI

Rozdziały pierwszego wydania

01. Poświadczenia weryfikowalne– wyjaśnienie

02. Poświadczenia weryfikowalne w działaniu

03. Metody zdecentralizowanych identyfikatorów (DID)

04. Tożsamość cyfrowa

05. Model zaufania wydawców tożsamości cyfrowej

06. OpenID Connect dla weryfikowalnych poświadczeń

07. Cyfrowe Portfele

Tożsamość cyfrowa – spis treści

Czego dowiesz się w tym rozdziale?

4.1

Jakie są różne podejścia do tożsamości cyfrowej?

4.2

Jakie jest podejście do pilotażowych przypadków użycia weryfikowalnych poświadczeń?

4.3

Jakie jest podsumowanie tych podejść?

4.1

**Jakie są różne podejścia
do tożsamości cyfrowej?**

Tożsamość cyfrowa jest fundamentem wszystkich innych usług cyfrowych

Łączy naszą tożsamość cyfrową z rzeczywistą tożsamością – np. edukacja, finanse, praca, zdrowie, świadczenia społeczne.



Trzy podejścia do tożsamości cyfrowej

Istnieją trzy główne podejścia do cyfrowej tożsamości:



Krajowe:

oparte na centralnym dostawcy tożsamości (np. rządowym systemie eID).

Federacyjne:

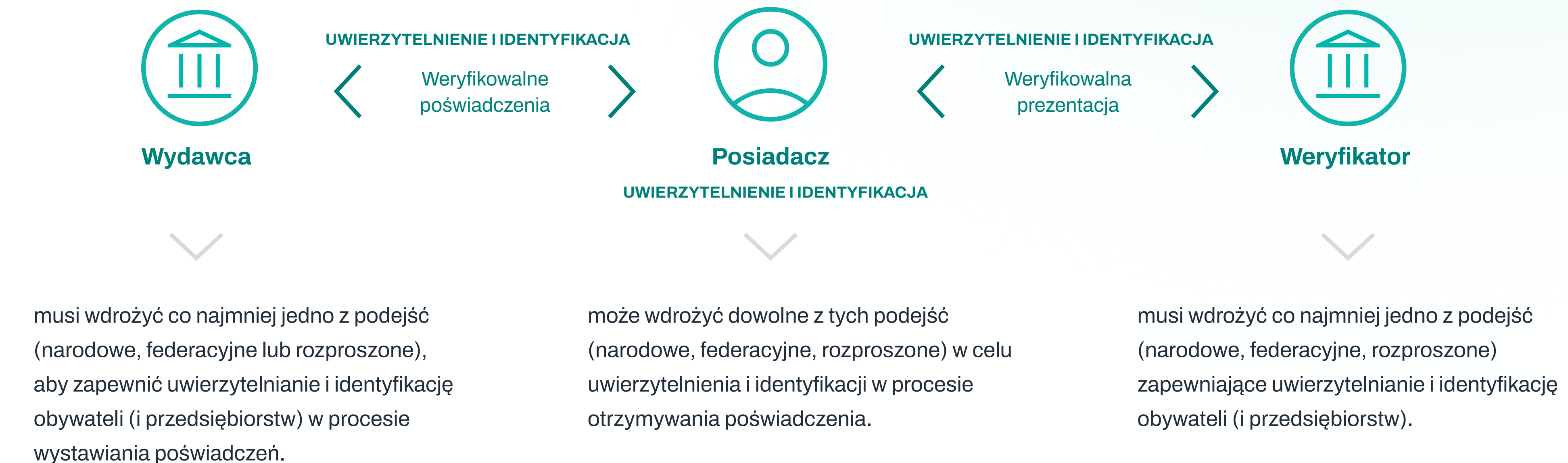
oparte na współpracy wielu dostawców tożsamości w kraju lub transgranicznie (np. eIDAS, logowanie przez sieci społecznościowe).

Samodzielnie zarządzane (SSI):

oparte na poświadczeniach weryfikowalnych (Verifiable Credentials) i zdecentralizowanym modelu, gdzie użytkownik sam kontroluje swoje dane i wybiera, co udostępnia.

Kiedy wymagane jest uwierzytelnianie i identyfikacja?

Uwierzytelnianie i identyfikacja są wymagane w aplikacjach używanych przez wystawców i weryfikatorów poświadczeń oraz wewnątrz samego portfela cyfrowego posiadacza.



* Gdy weryfikacja odbywa się osobiście zamiast online, identyfikację można przeprowadzić przy użyciu środków analogowych (np. dowodu osobistego).

4.2.

**Jak działają różne podejścia
do tożsamości cyfrowej?**

Krajowe podejście

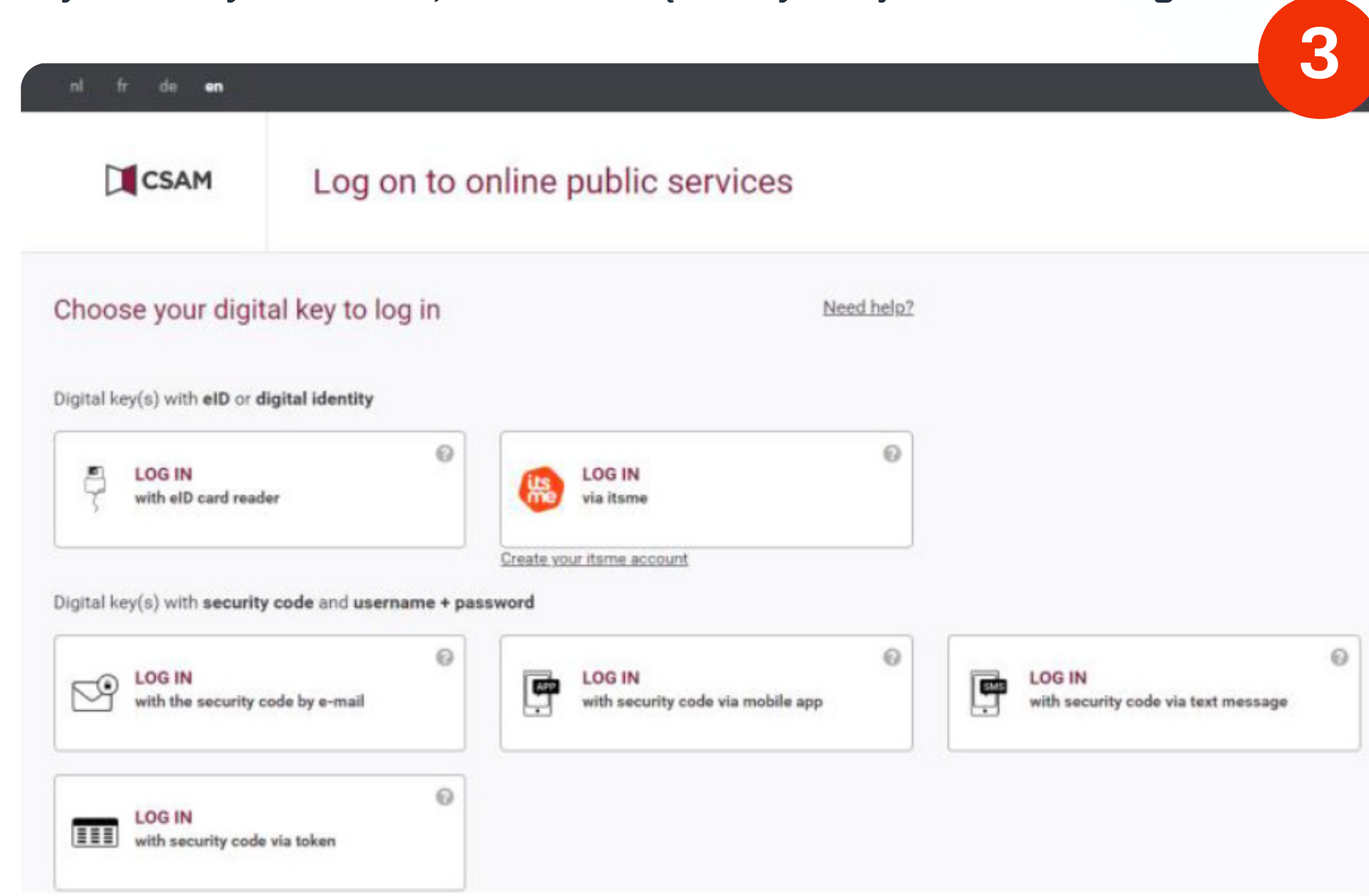


Centralny organ (np. państwo członkowskie)
zarządza krajową usługą tożsamości
odpowiedzialną za uwierzytelnianie
i identyfikację obywateli przy dostępie
do jego usług cyfrowych.

Krajowe podejście – Jak to działa?

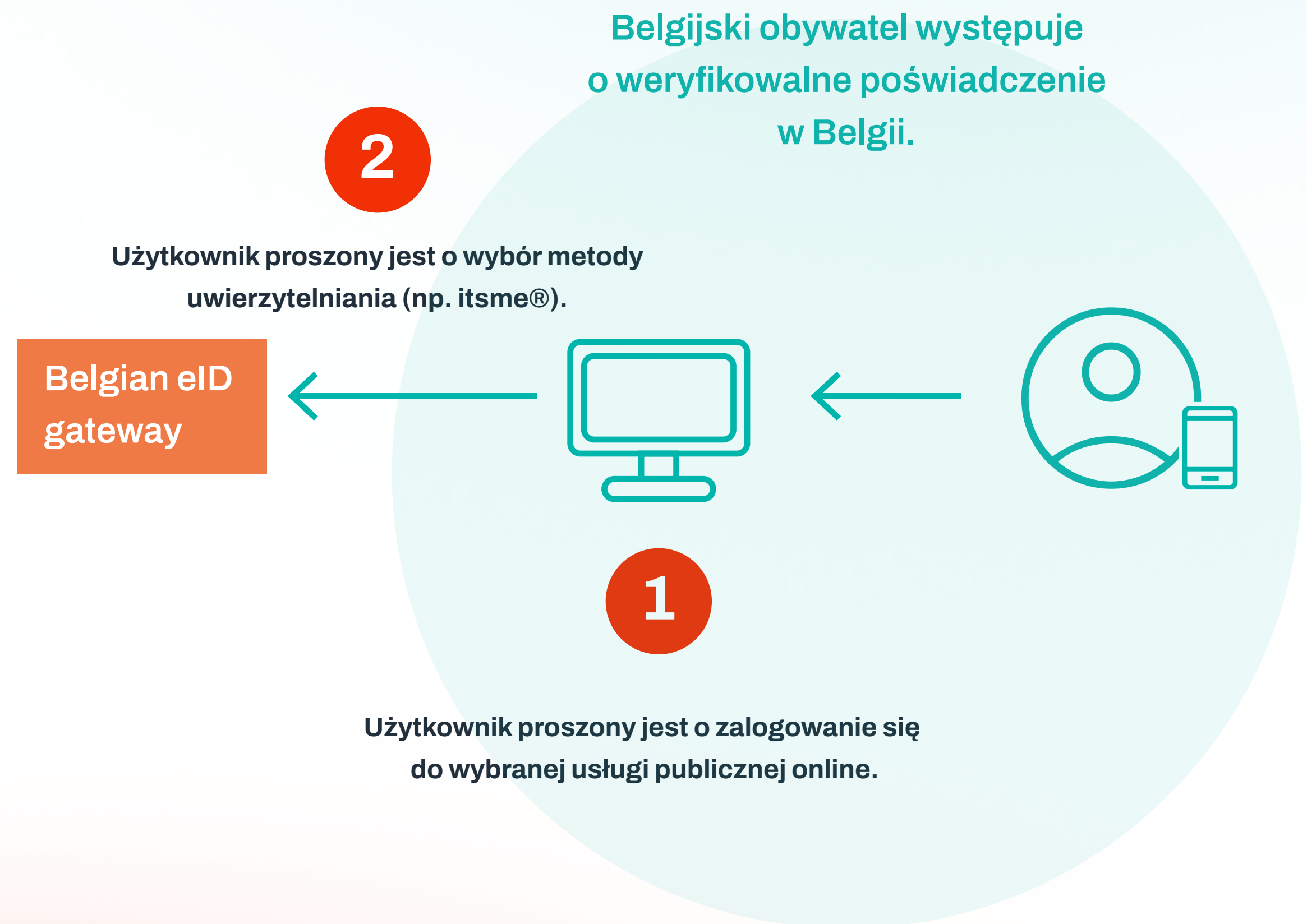
Przykład: użycie krajowych środków eID do uzyskania poświadczenia weryfikowalnego.

Użytkownik wybiera itsme®, mobilne rozwiązanie cyfrowej tożsamości w Belgii.



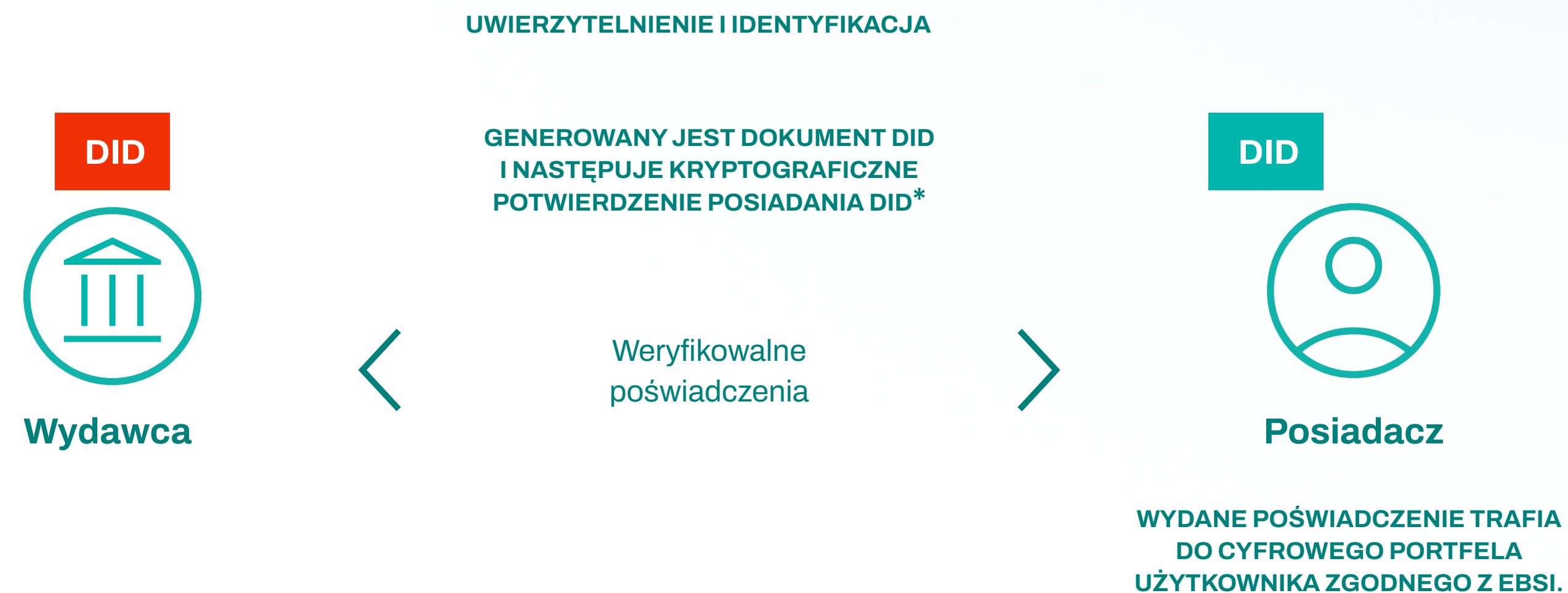
The screenshot shows the CSAM (Central Service Access Module) login interface. At the top, there are language options (nl, fr, de, en) and a red circle with the number 3. Below the header, it says 'Log on to online public services'. The main section is titled 'Choose your digital key to log in' with a 'Need help?' link. It is divided into two categories: 'Digital key(s) with eID or digital identity' and 'Digital key(s) with security code and username + password'. The first category includes 'LOG IN with eID card reader' and 'LOG IN via itsme' (with a 'Create your itsme account' link). The second category includes 'LOG IN with the security code by e-mail', 'LOG IN with security code via mobile app', 'LOG IN with security code via text message', and 'LOG IN with security code via token'.

CSAM jest bramą do zarządzania tożsamością i dostępem do usług publicznych rządu Belgii.



Po pomyślnym uwierzytelnieniu następuje wystawienie poświadczenia weryfikowalnego

Jeśli Posiadacz pomyślnie udowodnił własność DID przedstawionego Wydawcy



* Rozdział 3 wyjaśnia ten krok szczegółowo

Krajowe podejście – Korzyści dla obywatela



Mogę wybierać, jakie dane chcę ujawnić



Mogę wybierać dostawcę tożsamości



Mogę wybierać metodę uwierzytelniania



```
inflater: LayoutInflater, contain  
savedInstanceState: Bundle?  
): View {  
    mView = inflater.inflate(R.layout  
    initWebView()  
    return mView  
}  
@SuppressWarnings("SetJavaScriptEnabled")  
private fun initWebView() {  
    if (Build.VERSION.SDK_INT >= Build  
        WebView.setWebContentsDebuggi  
    }  
    mView.webViewLogin.clearCache(tr  
    mView.webViewLogin.clearHistory(  
    clearCookies(requireContext())  
}
```

00:00:15:09

mView.webViewLogin.setStrings(java
| o.s. 761237885 | 09

mView.webViewLogin.webViewClient

mView.loading

view.loadUrl

return

display : block}

overflow : hidden}

0 11 0 1

1 10 1001 01010110

1 0

10

13

0 11 0010

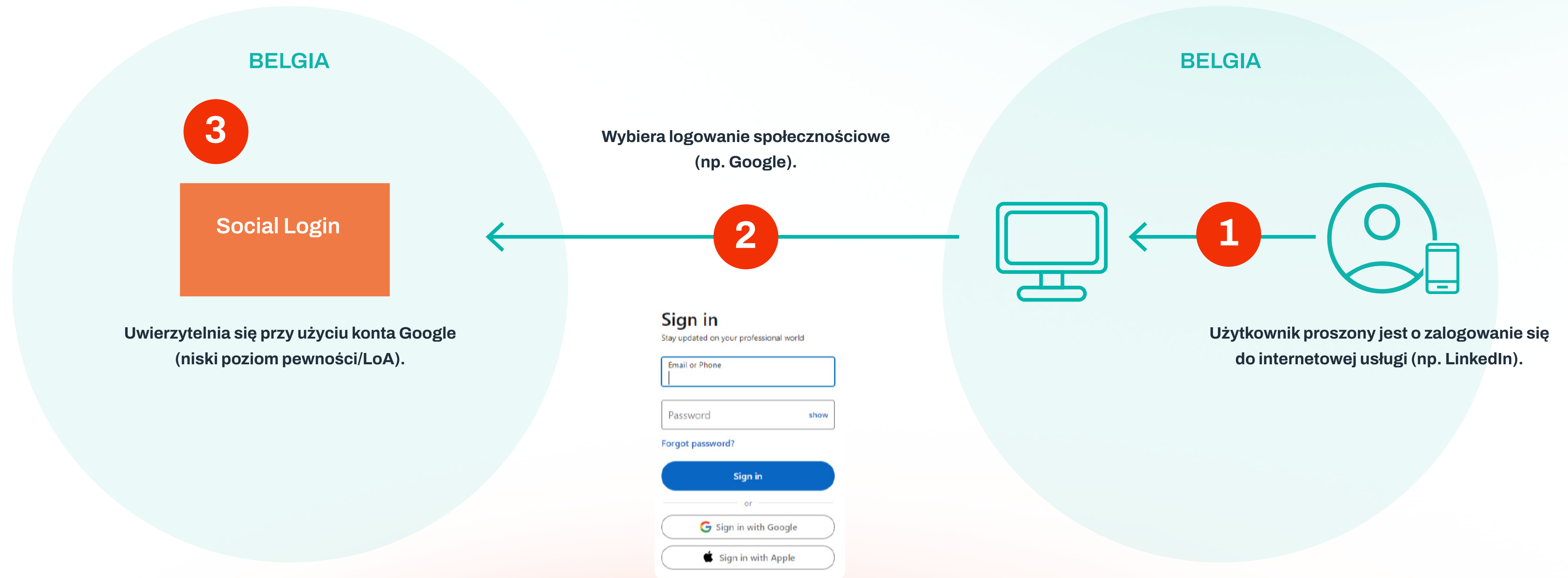
Federacyjne podejście

Podejście federacyjne zakłada współpracę wielu systemów tożsamości. Na przykład rozporządzenie eIDAS umożliwia wzajemne uznawanie krajowych systemów eID transgranicznie, co pozwala obywatelom używać krajowych eID w innych krajach UE.

Źródło: Rozporządzenie Parlamentu (UE) 2014/910 (eIDAS).

Federacyjne podejście – Jak to działa? (cz. 1/3)

Przykład: użycie eIDAS w scenariuszu transgranicznej weryfikacji.



Federacyjne podejście – Jak to działa? (cz. 2/3)

Przykład: użycie eIDAS w scenariuszu transgranicznej weryfikacji.

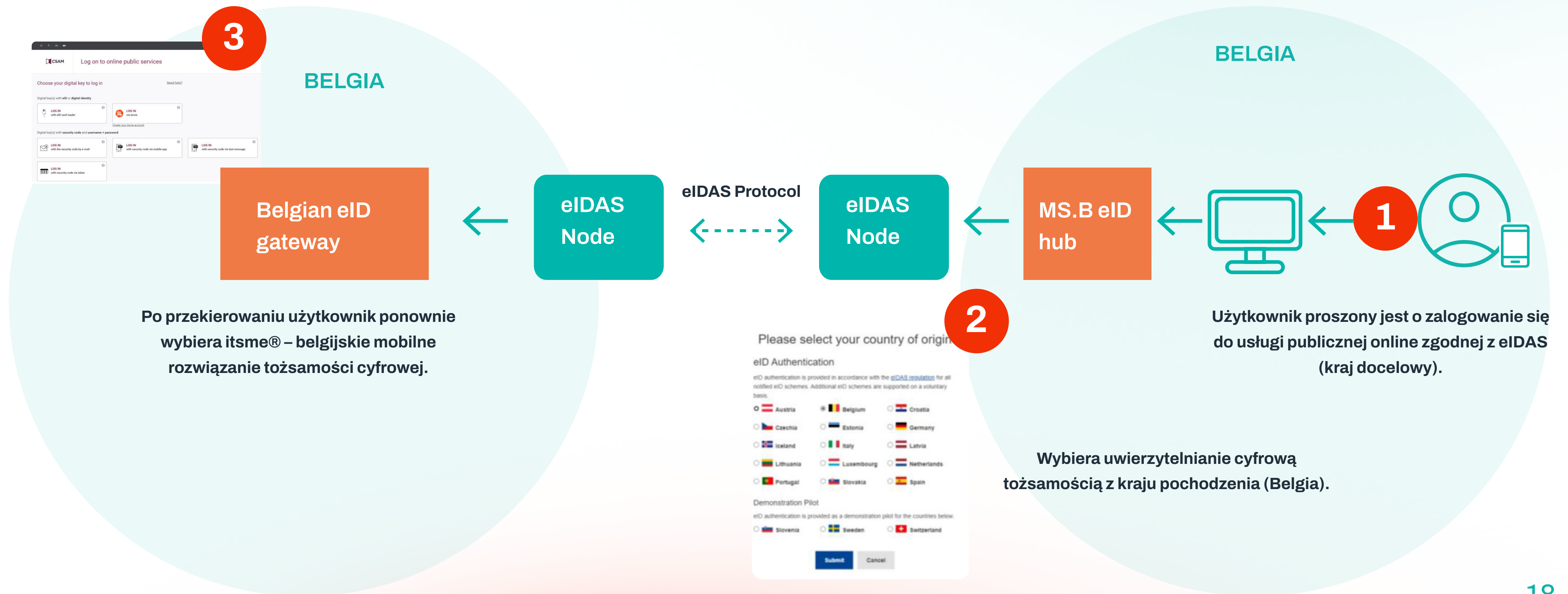
Podejście federacyjne w kraju: kilku dostawców tożsamości (narodowych i sektorowych) współpracuje w ramach krajowego systemu.



Federacyjne podejście – Jak to działa? (cz. 3/3)

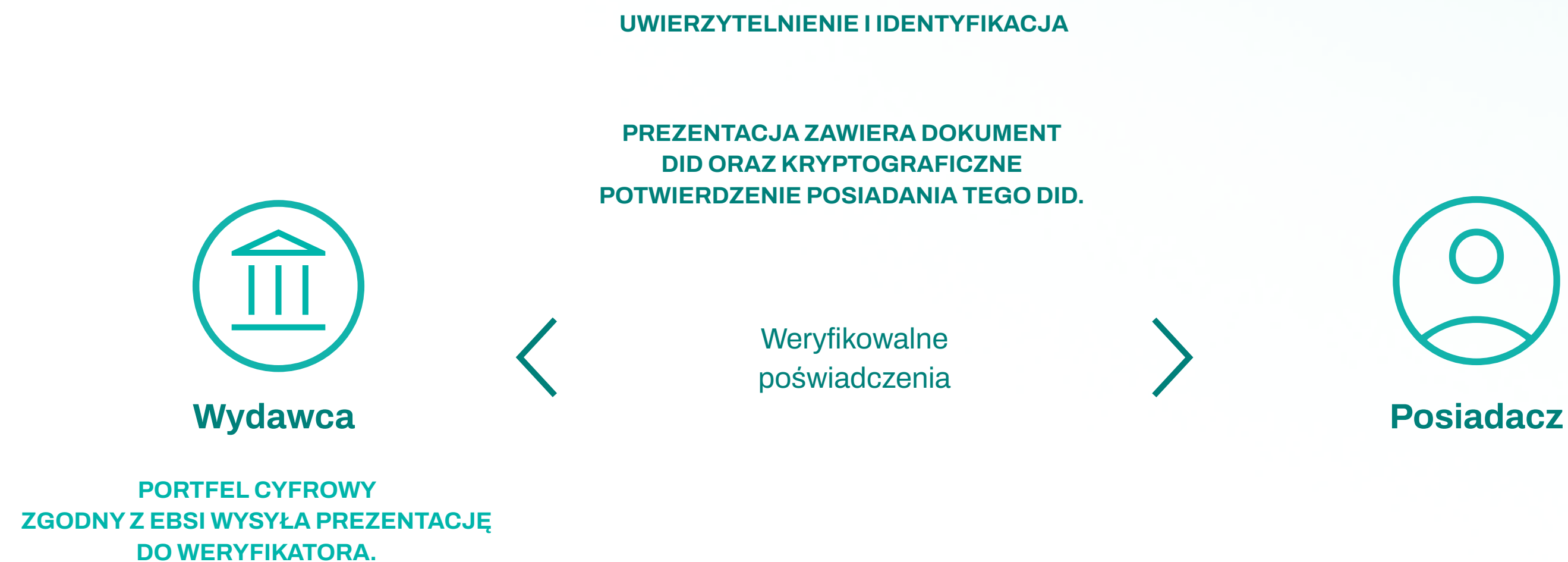
Przykład: użycie eIDAS w scenariuszu transgranicznej weryfikacji.

Uwierzytelnianie transgraniczne (eIDAS)



Po pomyślnym uwierzytelnieniu udostępniana jest weryfikowalna prezentacja

Jeśli Posiadacz (Holder) pomyślnie udowodnił własność DID przedstawionego Wydawcy



* Rozdział 3 wyjaśnia ten krok szczegółowo

Federacyjne podejście – Korzyści dla obywatela



Mogę wybierać, jakie dane chcę ujawnić.

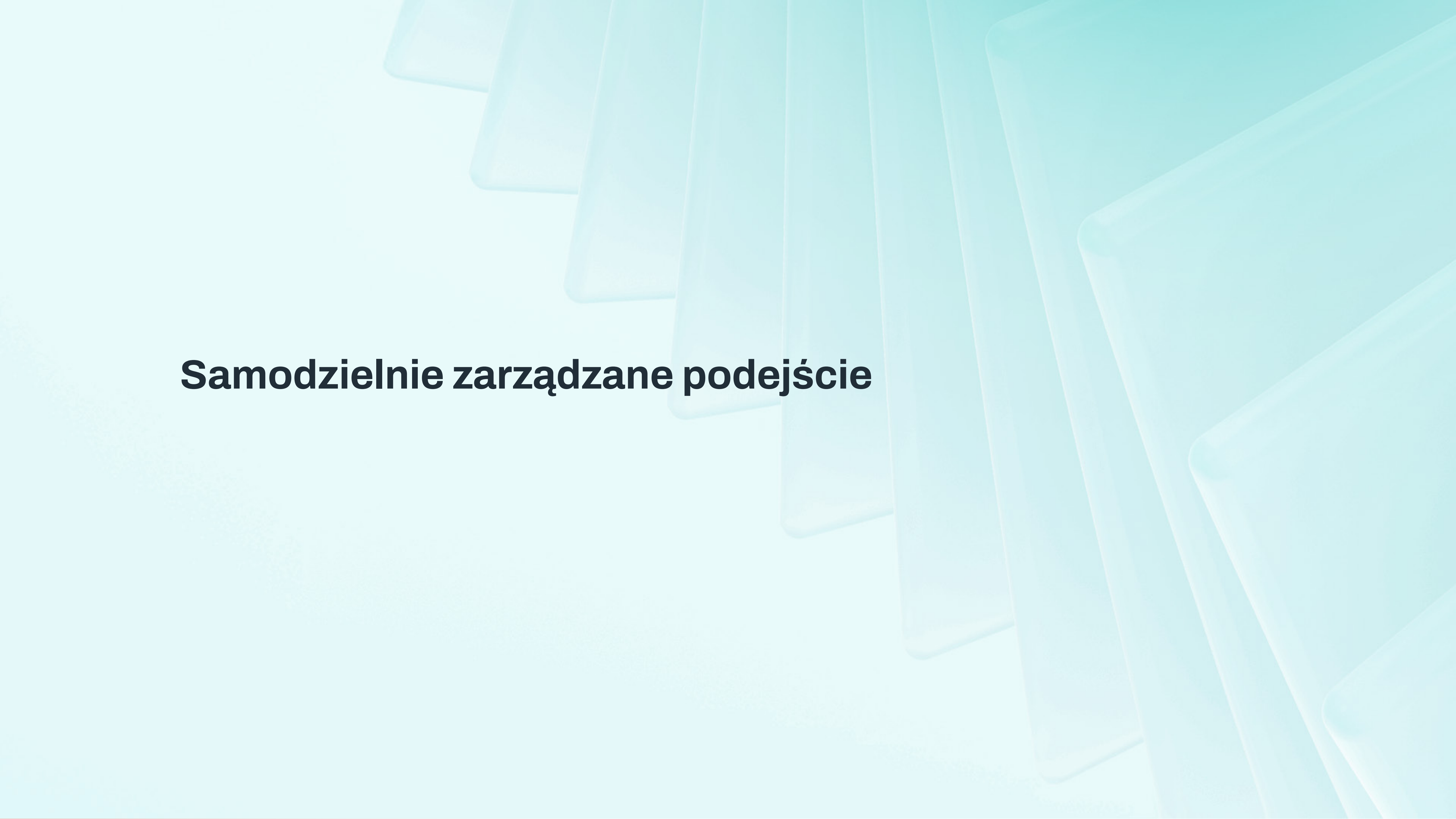


Mogę wybierać dostawcę tożsamości.



Mogę wybierać metodę uwierzytelniania.





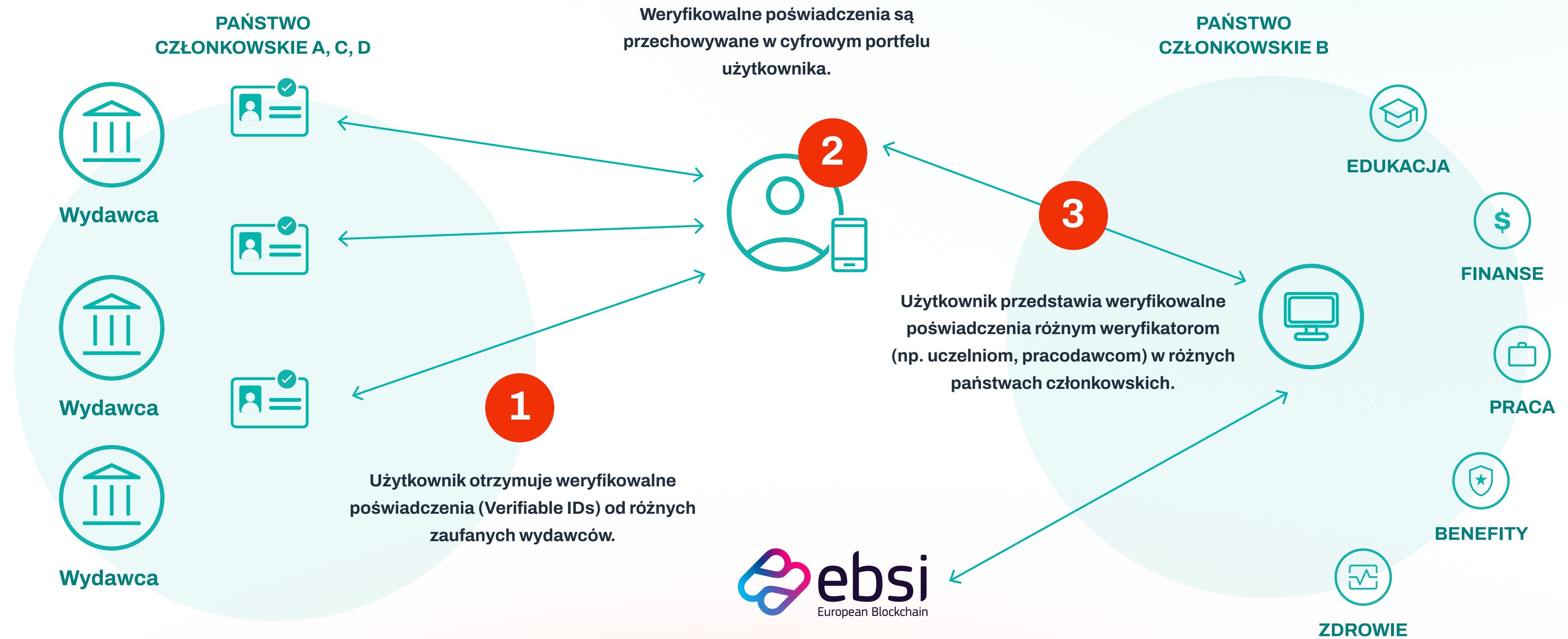
Samodzielnie zarządzane podejście

Samodzielnie zarządzana tożsamość cyfrowa opiera się na modelu, w którym użytkownik sam kontroluje swoje poświadczenia w zdecentralizowanym portfelu cyfrowym. W3C Verifiable Credentials można wykorzystać do tworzenia **weryfikowalnych tożsamości cyfrowych** (Verifiable IDs), które łatwo łączy się z innymi poświadczeniami w celu rozszerzenia liczby atrybutów używanych do uwierzytelniania i identyfikacji oraz do dopasowywania danych. Model ten wspiera także wystawianie i prezentację weryfikowalnych zaświadczeń (Verifiable Attestations).



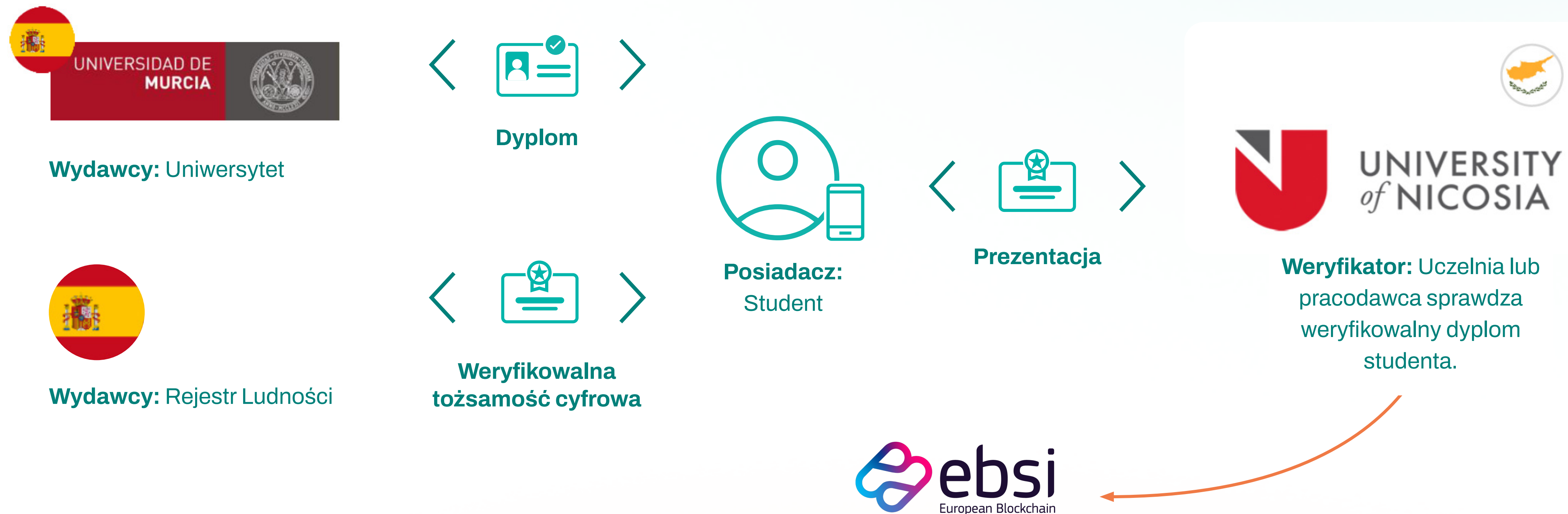
Samodzielnie zarządzane podejście – Jak to działa?

Przykład: Inicjatywa ESSIF (European Self-Sovereign Identity) w ramach EBSI



EBSI Multi-University – przykład samodzielnego zarządzania

Pilotaż Multi-University: użycie Verifiable ID (weryfikowalnej tożsamości cyfrowej) i Verifiable Diploma (weryfikowalnego dyplomu).



Proces: Student używa swojego portfela cyfrowego do przedstawienia weryfikowalnego dyplomu (poświadczenia), które weryfikator potwierdza jako autentyczne i wydane przez zaufanego wystawcę.

Samodzielnie zarządzanie – Korzyści dla obywatela



Mogę wybierać, jakie dane chcę ujawnić.



Mogę wybierać dostawcę tożsamości.



Mogę wybierać metodę uwierzytelniania.



Zarządzanie tożsamością – Portfele

Użytkownik może używać dowolnego portfela cyfrowego do uwierzytelniania i otrzymywania poświadczeń.

Model zdecentralizowany umożliwia posiadaczom wybór portfela i kontrolę nad udostępnianymi poświadczeniami. Obecnie 13 portfeli jest zgodnych ze specyfikacjami EBSI (kolejne są w fazie wdrożenia).

DESKTOP


MOBILE


DESKTOP & MOBILE




4.3.

**Jakie jest podsumowanie
tych podejść?**

Podsumowanie podejść

	Krajowe:	Federacyjne:	Samodzielnie zarządzane:
	Centralny organ (rząd) zarządza usługą tożsamości (np. eID na kartach elektronicznych). Stosuje standardy takie jak SAML i wspólny zestaw danych eIDAS.	Krajowe węzły (np. w ramach eIDAS) łączą dostawców tożsamości, umożliwiając transgraniczne uwierzytelnianie. Zapewnia interoperacyjność między systemami.	Wykorzystuje Verifiable Credentials do tworzenia i weryfikowania cyfrowych tożsamości (Verifiable IDs). Zapewnia elastyczne ujawnianie informacji, łatwe łączenie poświadczeń oraz współpracę z portfelami cyfrowymi.
Przykład:	system CSAM w Belgii.	europejska sieć eIDAS.	ESSIF (EBSI). Uwaga: nie przechowuje danych osobowych w łańcuchu bloków (on-chain).
Mocne strony:	państwowa kontrola nad usługą, prosta integracja z krajowymi systemami.	interoperacyjność i uwierzytelnianie transgraniczne (eIDAS).	selektywne ujawnianie danych, łatwość łączenia z innymi poświadczeniami, obsługa portfeli cyfrowych.

Wartość dla poszczególnych podmiotów

	Podejście krajowe	Podejście federacyjne:	Podejście samzarządzania poświadczeniami
Wystawca	Niezawodne uwierzytelnianie i identyfikacja obywateli państw członkowskich	Przydatne w przypadku uwierzytelniania transgranicznego	Może być używane w połączeniu z innymi metodami uwierzytelniania i poświadczeniami weryfikowalnymi
Portfel	Prosta integracja z usługami krajowymi	Przydatne w przypadku uwierzytelniania transgranicznego	Przydatne dla uwierzytelniania transgranicznego i wymiany poświadczeń weryfikowalnych
Weryfikator	Niezawodne źródła informacji	Przydatne dla zastosowań transgranicznych	Przydatne do szybkiej i niezawodnej weryfikacji poświadczeń weryfikowalnych

Chcesz dowiedzieć się więcej?

Najważniejsze źródła

Strona internetowa EBSI

<https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Home>

Podręcznik poświadczeń weryfikowalnych EBSI

<https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/EBSI+Verifiable+Credentials+Playbook>

Demonstracje EBSI (Demo Day)

<https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/EBSI+Demo+Day>

