eIDAS odstartuje Německo

Jaromír Talíř • jaromir.talir@nic.cz • 24. 11. 2017

Obsah

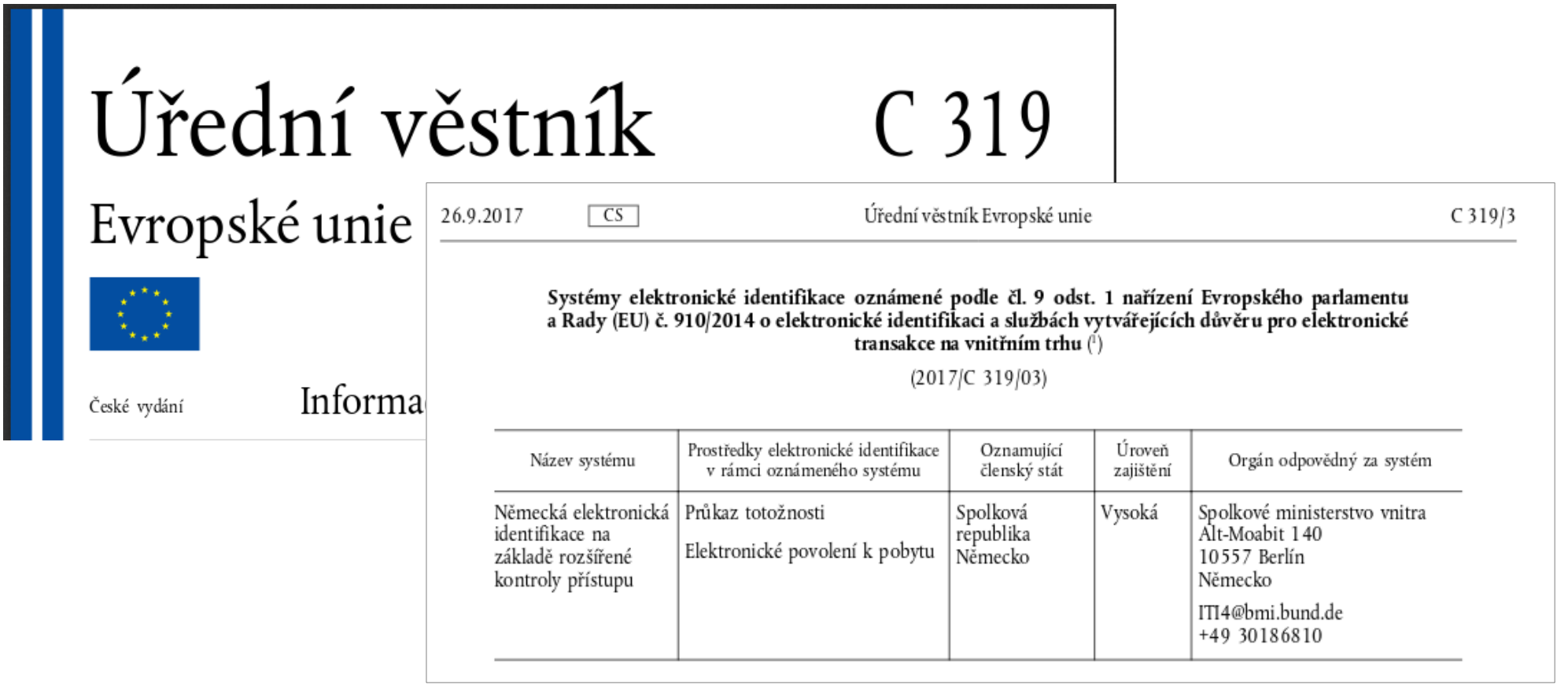
- Vzájemné uznávání eID podle eIDAS
- Německá elektronická identifikace
- Nové německé eID systémy
  - DomainID
  - Verimi

Vzájemné uznávání eID podle eIDAS

- Místní veřejné online služby, které využívají elektronickou identifikaci se značnou nebo vysokou úrovní záruky, musí umožnit přihlášení pomocí **oznámených** eID systémů ostatních členských států
- Zatím není jasné, kterých služeb se to bude týkat

Září 2018						
po	út	st	čt	pá	so	ne
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

První oznámený eID systém - Německo



Úřední věstník C 319

Evropské unie

České vydání Informa

Systémy elektronické identifikace oznámené podle čl. 9 odst. 1 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu ([1])

(2017/C 319/03)

Název systému	Prostředky elektronické identifikace v rámci oznámeného systému	Oznamující členský stát	Úroveň zajištění	Orgán odpovědný za systém
Německá elektronická identifikace na základě rozšířené kontroly přístupu	Průkaz totožnosti Elektronické povolení k pobytu	Spolková republika Německo	Vysoká	Spolkové ministerstvo vnitra Alt-Moabit 140 10557 Berlín Německo ITI4@bmi.bund.de +49 30186810

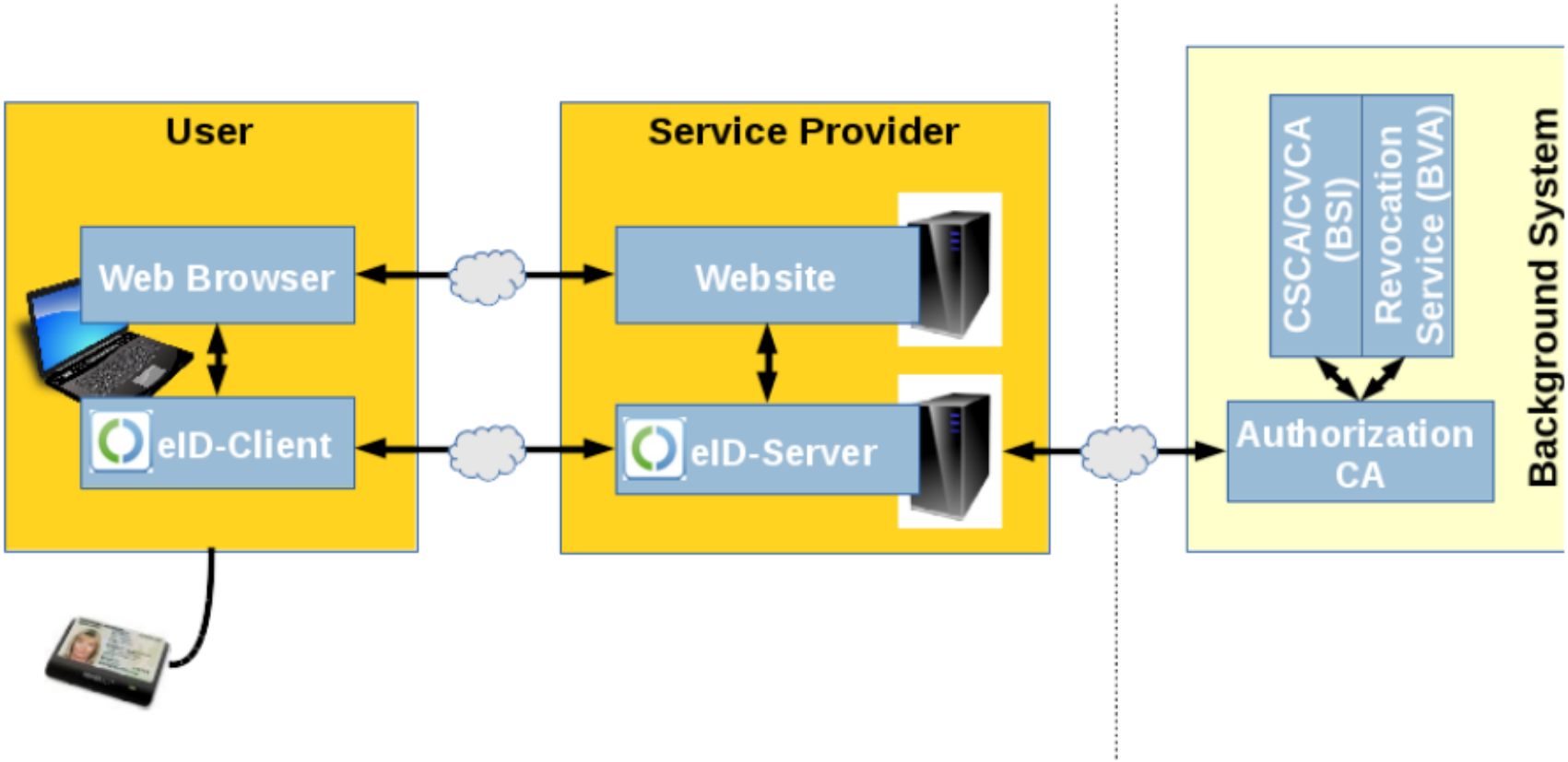
Německá elektronická identifikace

- Spuštěno v 11/2010
- Přes 51 mil. karet v oběhu (Německo má 83 mil. Obyvatel)
  - Zhruba 1/3 aktivovaných (před 06/2017 opt-in, nyní opt-out)
  - Bezkontaktní čip + 6ti číselný PIN
- 157 poskytovatelů (2/3 veřejný sektor, 1/3 soukromý sektor)
- Decentralizovaná architektura
  - Neexistuje centrální server, který by ověřoval autentizaci a poskytoval data => osobní údaje jsou přímo na kartě

Německá elektronická identifikace - karta

Přijmení	Rodné příjmení*	Jméno
Titul*	Datum narození	Místo narození
Adresa	Typ dokumentu	Datum expirace
Identifikátor	Identifikátor specifický pro službu	Věk je více/méně než?
Adresa odpovídá místu?	Církevní jméno/ umělecké jméno*	Označené * jsou volitelné

Německá elektronická identifikace - schéma



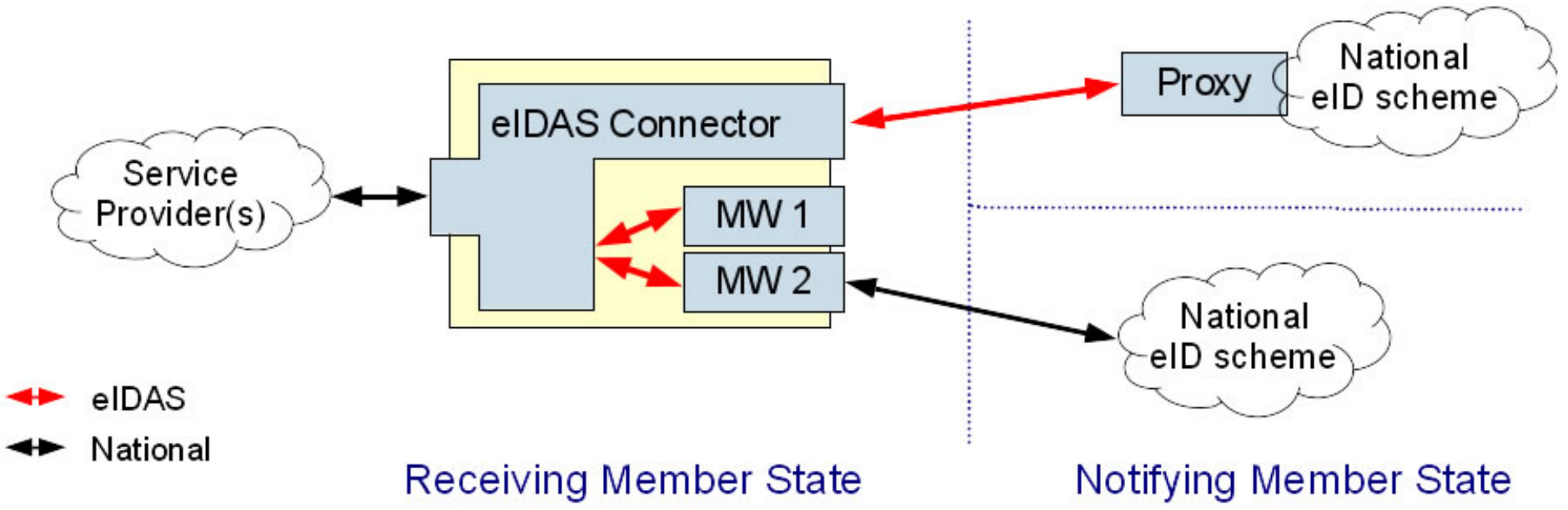
Německá elektronická identifikace - klienti

- Oficiální klient AusweisApp 2
  - https://www.ausweisapp.bund.de/en/ausweisapp2-home/
  - Windows, OS X, Android a iOS (beta)
  - Zdrojové kódy od 07/2017 na GitHubu
- Neoficiální klient Open eCard
  - https://www.openecard.org/en/startpage/
  - Java

Německá elektronická identifikace - čtečky

- Mobilní telefony
  - NFC musí podporovat „Extended Length“
  - Ani Google Nexus řada, ani Pixel
- Externí NFC čtečka karet
  - Jediný oficiálně podporovaný typ je **REINER SCT cyberJack wave** za cca 100 EUR na Amazonu

Německá elektronická identifikace - eIDAS



Nové německé eID projekty - DomainID

- Projekt, za kterým stojí německý správce domény DENIC
- Motivace pro realizaci jsou podobné jako u mojeID
- Prvně veřejně prezentováno v říjnu, spuštění v plánu na 2018
- Postavené nad protokolem OpenID Connect
  - Oddělená správa autentizace a údajů o identitě
  - Snaha a poskytnutí ověřené informace o vlastnictví domény
  - Modifikovaný „discovery“ proces

Nové německé eID projekty - DomainID

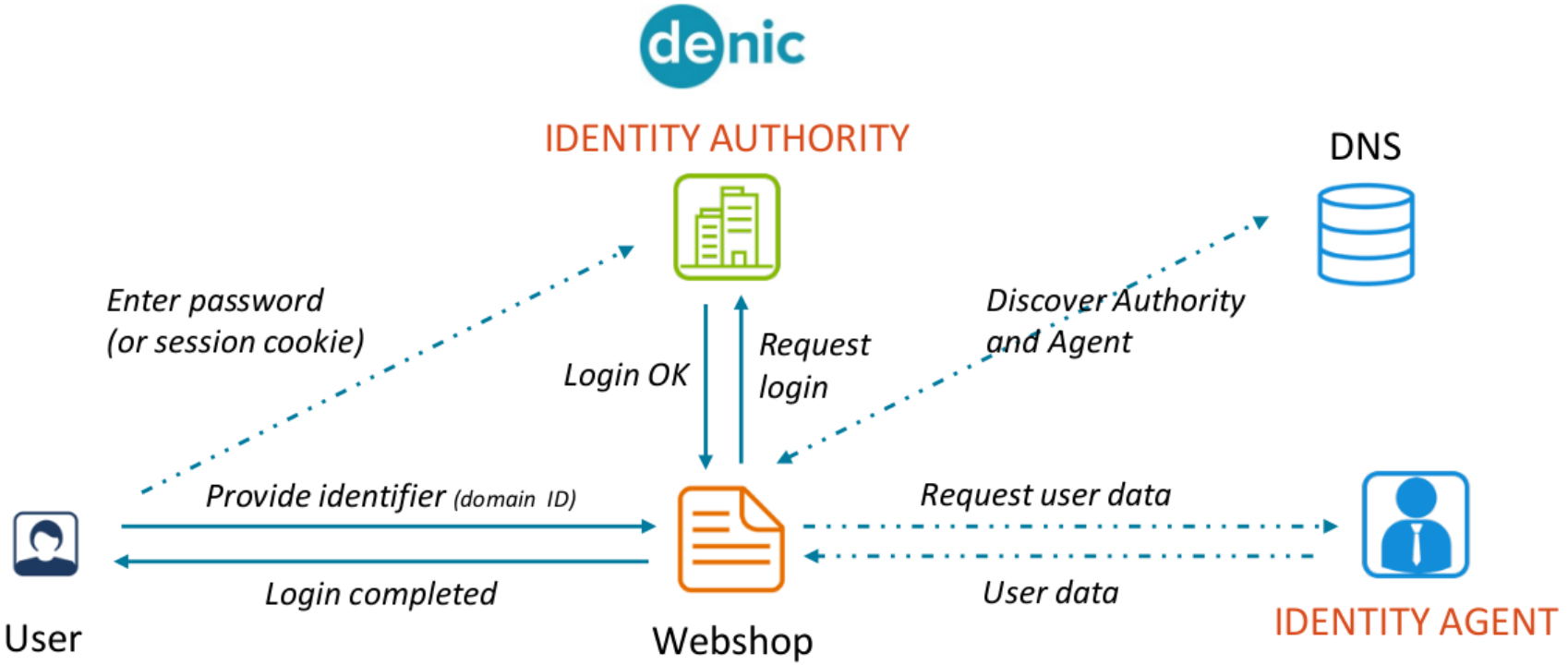
- Oddělená správa přihlášení a předání údajů
  - Identity Authority (iau) a Identity Agent (iag)
  - Rozdělení kopíruje vztah Registr a Registrátor
  - Využívá vlastnost OpenID Connect zvanou „distributed claims“
- Kontrola vlastnictví domény
  - Předpokládá použití ACME
  - Komplikuje integraci existujících identitních poskytovatelů

Nové německé eID projekty - DomainID

- OpenID Connect discovery
  - Proces, který ze zadaného identifikátoru získá informaci o OpenID Connect serveru obsluhujícím odpovídající identitu
  - Využívá protokolu WebFinger, který vyžaduje HTTP/S komunikaci se serverem - identifikátor může být ve tvaru domény nebo e-mailu
- DomainID discovery
  - Identifikátor je doména, využívá se pouze DNS(SEC)

```
$ dig TXT _domainid.jara.talir.cz +short
"v=DID1;iau=auth.freedom-id.de;iag=identityagent.de"
```

Nové německé eID projekty - DomainID



Nové německé eID projekty - DomainID

- Protokol a zároveň služba provozovaná v DENIC
- Možné propojení s mojeID
- Problém bude získat poskytovatele služeb, kteří implementují přihlášení
- Registrace DomainID: https://auth.freedom-id.de/domain-id
- Ukázkový poskytovatel služby: https://shop.freedom-id.de/

Nové německé eID projekty - Verimi

- Projekt za kterým stojí komerční společnosti
  - T-Mobile, Lufthansa, Deutche bank, Allianz, ...
- Oznámeno v srpnu, spuštěno má být na přelomu 2017/2018
  - Zatím je možné se pouze zaregistrovat na https://verimi.de/
- Zveřejněná dokumentace
- Zveřejněno testovací prostředí

Nové německé eID projekty - Verimi

- Jednotné přihlašování přes OpenID Connect
  - Podpora dvoufaktorové autentizace
  - Registrace ověřených údajů (pas, občanský průkaz) na základě video identifikace
- Verimi API pro přístup k údajům identit zabezpečené OAuth 2
- „Platební funkce“ - bez bližší specifikace

Shrnutí

- „Exploze“ úprav existujících a nových projektů v oblasti elektronické identifikace v Německu v roce 2017
- Německá e-občanka je komplikovaná jak pro uživatele tak pro poskytovatele služeb
  - Na druhou stranu snaží se jít cestou podpory open source
- Jeden z největších doménových registrů světa následuje vizi nastartovanou námi před sedmi lety projektem mojeID

Děkuji za pozornost

Jaromír Talíř • jaromir.talir@nic.cz

CZ.PEPS
CZECH REPUBLIC PAN-EUROPEAN PROXY SERVICES
Spolufinancováno Evropskou unií
Nástroj pro propojení Evropy