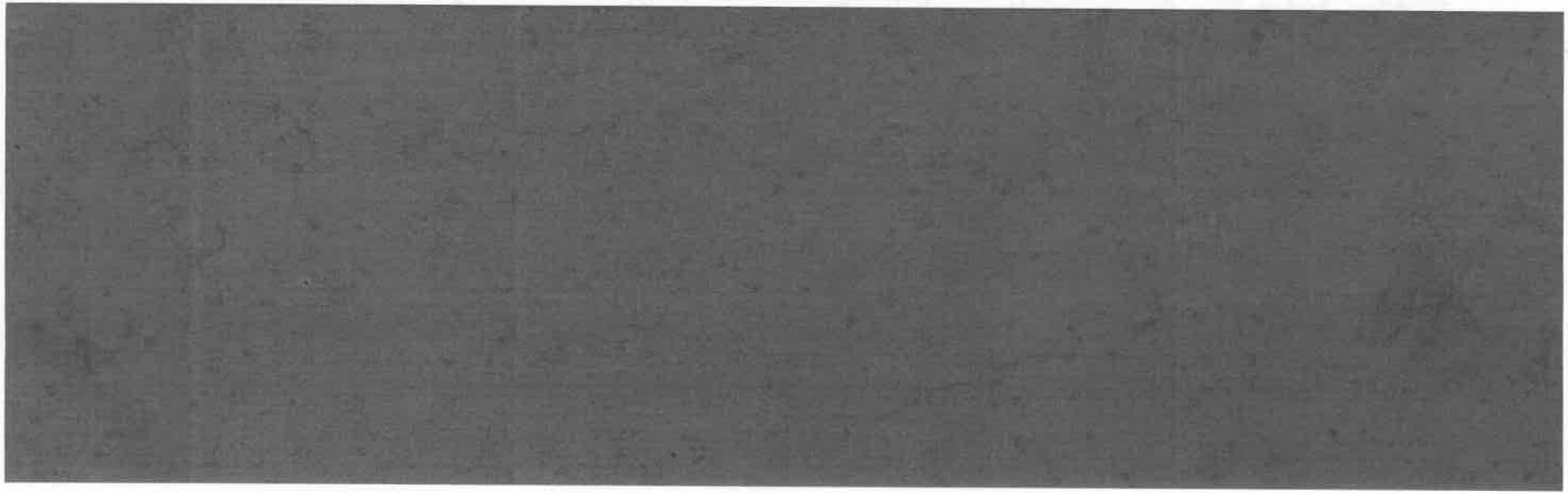
Bundesverwaltungsamt

Alternative zur Umsetzung des IDNrG

Domänen-ID-Modell



Anforderungen

Ein alternatives Modell muss die folgenden Anforderungen erfüllen:

- Sehr hoher Datenschutz
- Keine Verwendung der Steuer-ID als zentrale ID, stattdessen beliebige Bereichs-/Domänenspezifische IDs
- Daten zur Person liegen nur bei einer zentralen Stelle (BZSt)
- Beibehaltung der bestehenden Prozesse zur Datenpflege zwischen Meldebehörden und BZSt
- Verbesserung der Datenqualität in den Registern (Verwendung BZSt-Daten)
- Unterstützung des registergestützten Zensus
- Hohe Flexibilität für künftige Anforderungen (eID, EU, ...)
- Nutzung vorhandener Infrastrukturen möglich (z.B. DVDV, PKI)
- Geringe Anpassungen im Gesetzentwurf
- Überschaubarer Mehraufwand (für alle Beteiligten)
- Keine deutliche Mehrbelastung für BZSt (gem. Vereinbarung mit BMF)

Lösungsansatz Domänen-ID-Modell

Hoher Datenschutz, geringe Komplexität und große Flexibilität

Zentrale Steuer-ID

- Vorteile durch einfache Umsetzung
- Politische Fragen zum Datenschutz

Domänen-ID-Modell

- Einfache Umsetzung
- Hoher Datenschutz
- Zukunftssicher

Österreichisches Modell

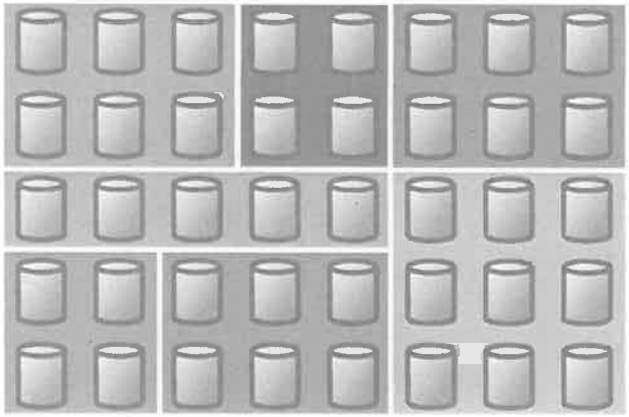
- Nachteile durch komplexe Umsetzung
- Vorteile im Bereich des Datenschutzes

Kernaspekte

1. Domänen-IDs
2. Geschützte Übersetzungstabelle
3. Verschlüsselte IDs

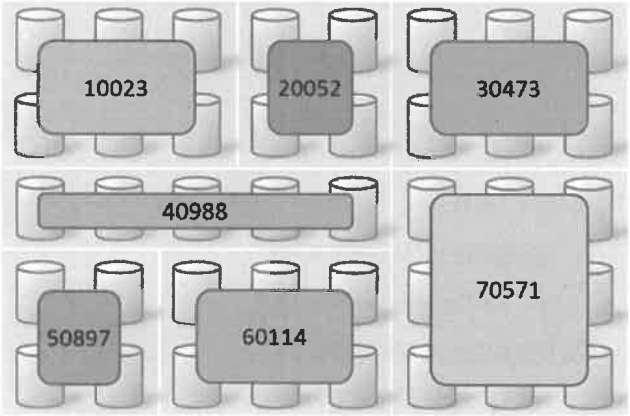
Domänen-ID

Die Register werden in beliebig viele unterschiedliche Bereiche (Domänen*) aufgeteilt. Jedes Register kann grundsätzlich nur zu einer Domäne gehören.



In jeder Domäne wird jeder Person in allen Registern eine eindeutige (nicht-sprechende) Domänen-ID zugeordnet.

Dabei kann es sich um bereits vorhandene oder neu vergebene IDs handeln (geringer Aufwand bei vorhandenen IDs).

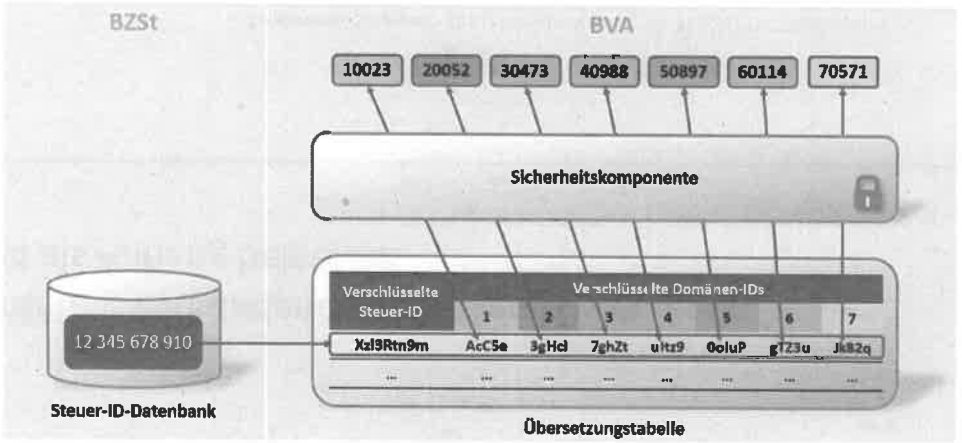


* z.B. NPA/eID, Renten, Steuern, Ausländer, Waffen, Arbeit, Soziales ...

Domänen-ID

Beim BVA wird eine Datei verwaltet, in der die Domänen-IDs zu jeder Personen verschlüsselt eingetragen werden.

Leere Felder werden mit Pseudo-IDs gefüllt, so dass für Menschen nicht ersichtlich ist, ob in einer Domäne tatsächlich Einträge vorhanden sind.

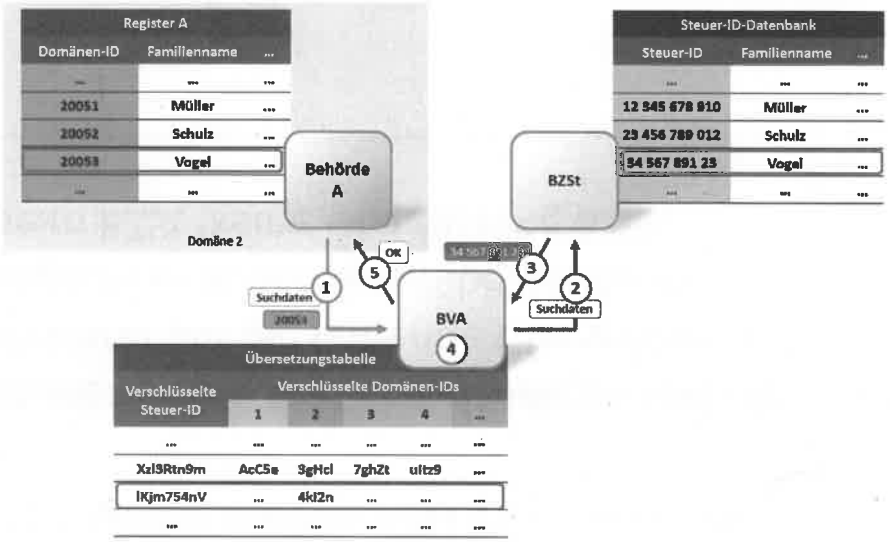


Hintergrund:

- Die Kommunikation zwischen Domänen setzt immer voraus, dass an einer Stelle eine Übersetzung erfolgen muss.
- Die vorgestellte Alternative trennt die Domänen sowie die Personendaten und die übersetzende Stelle strikt voneinander, verzichtet auf die laufende Übermittlung von Personendaten bei Anfragen und ermöglicht eine domänenübergreifende Kommunikation ohne ständige Abfragen beim BZSt (keine Überlastung BZSt).

Erstbefüllung / Aktualisierung

- Bei der Erstbefüllung werden im Register vorliegende Daten - wie im RegMoG vorgesehen - über BVA mit dem Datenbestand des BZSt abgeglichen.
- Bei eindeutiger Zuordnung werden die Domänen-ID und die Steuer-ID verschlüsselt gespeichert, so dass künftig Datenabrufe über die Domänen-ID möglich sind.

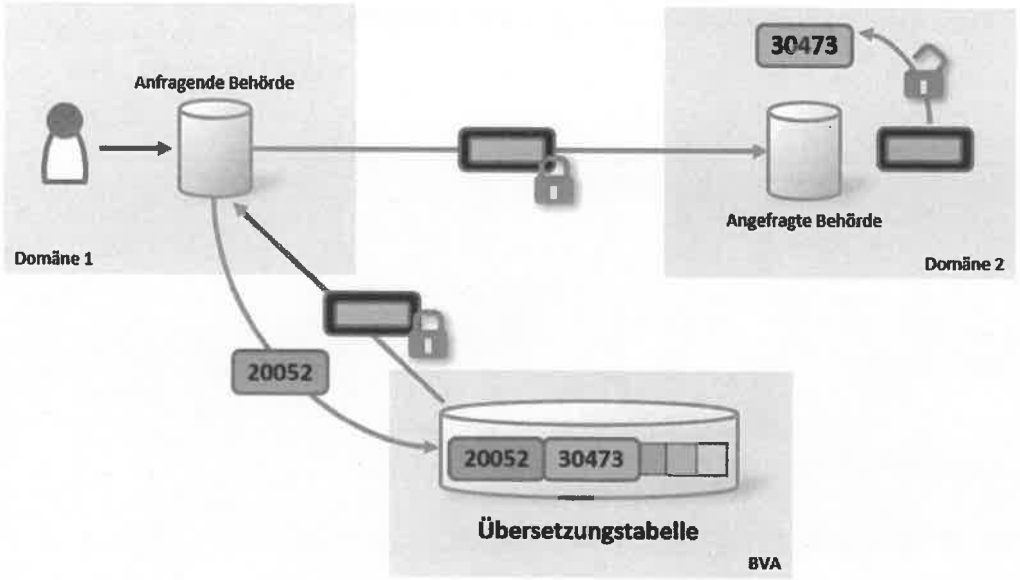


- BVA liefert eine entsprechende Rückmeldung (und - in dem im RegMoG vorgesehenen Rahmen - die zur Person beim BZSt vorliegenden Daten).

Detailbeschreibungen zur Erstbefüllung, Zuordnung vorhandener Domänen-IDs und der domänenübergreifenden Kommunikation sind als Anhang beigefügt.

Zielbild Kommunikation

- Eine Behörde übermittelt die Anfrage nach einer anderen Domänen-ID an das BVA.
- Vor einer Rückmeldung prüft BVA, ob tatsächlich eine Abfrageberechtigung besteht (zentrale Vermittlungsstelle, ggf. künftig auch Prüfung gegen Consentmodul)



- Die anfragende Behörde erhält eine temporär gültige, verschlüsselte Antwort, die nur von der angefragten Behörde aufgelöst werden kann.
- Die angefragte Behörde entschlüsselt die Anfrage, verfügt damit über die eigene Domänen-ID und übermittelt eine entsprechende Antwort.
- Ergänzend könnte die Kommunikation zwischen den beiden Domänen über das 4-Corner-Modell erfolgen (also doppelte Prüfung durch BVA und dezentrale Vermittlungsstellen).

Vorteile der Lösung

	Datenschutz	Wiederverwendung	Flexibilität
	• Domänenübergreifende Profilbildung durch Zusammenführen von Registerbeständen ist nicht möglich • BVA ist für alle bereichsübergreifenden Kommunikationen die im RegMoG geforderte „Dritte Stelle“	• Innerhalb einer Domäne werden bestehende IDs und etablierte Kommunikationsbeziehungen weiter genutzt: – Die Steuer-ID wird als Domänen-ID weiterverwendet – In anderen Domänen können andere IDs weiterverwendet werden (die Steuer-ID muss nicht eingeführt werden) – Die Datenbestände und Prozesse des BZSt können weiter genutzt werden	• Maximale Flexibilität bei Definition der Domänen: – Beliebige Anzahl an Domänen – Neue Domänen (EU, eID...) können jederzeit hinzugenommen werden – Auch dem Bürger könnte zu seiner Identifizierung bei der Antragstellung eine einheitliche digitale ID angeboten werden – Es können beliebig viele Bereiche definiert werden. Diese können sowohl etablierte IDs als auch neue IDs als Domänen-ID verwenden
. Geschützte Übersetzungstabelle			
	• Domänenübergreifende Profilbildung durch Zusammenführen der Übersetzungstabelle mit Registerbeständen ist nicht möglich • Tabelle nur bei einer Stelle, die strikt kontrolliert werden kann		• Die Dritte Stelle muss nur bei bereichsübergreifender Kommunikation involviert werden • Legitimierte Zusammenführung mehrerer Domänen möglich (z.B. Zensus-ID)
. Verschlüsselte Fremd-IDs			
	• Profilbildung durch schrittweises Mitschneiden der Domänen-ID anderer Domänen ist nicht möglich.		

Fazit

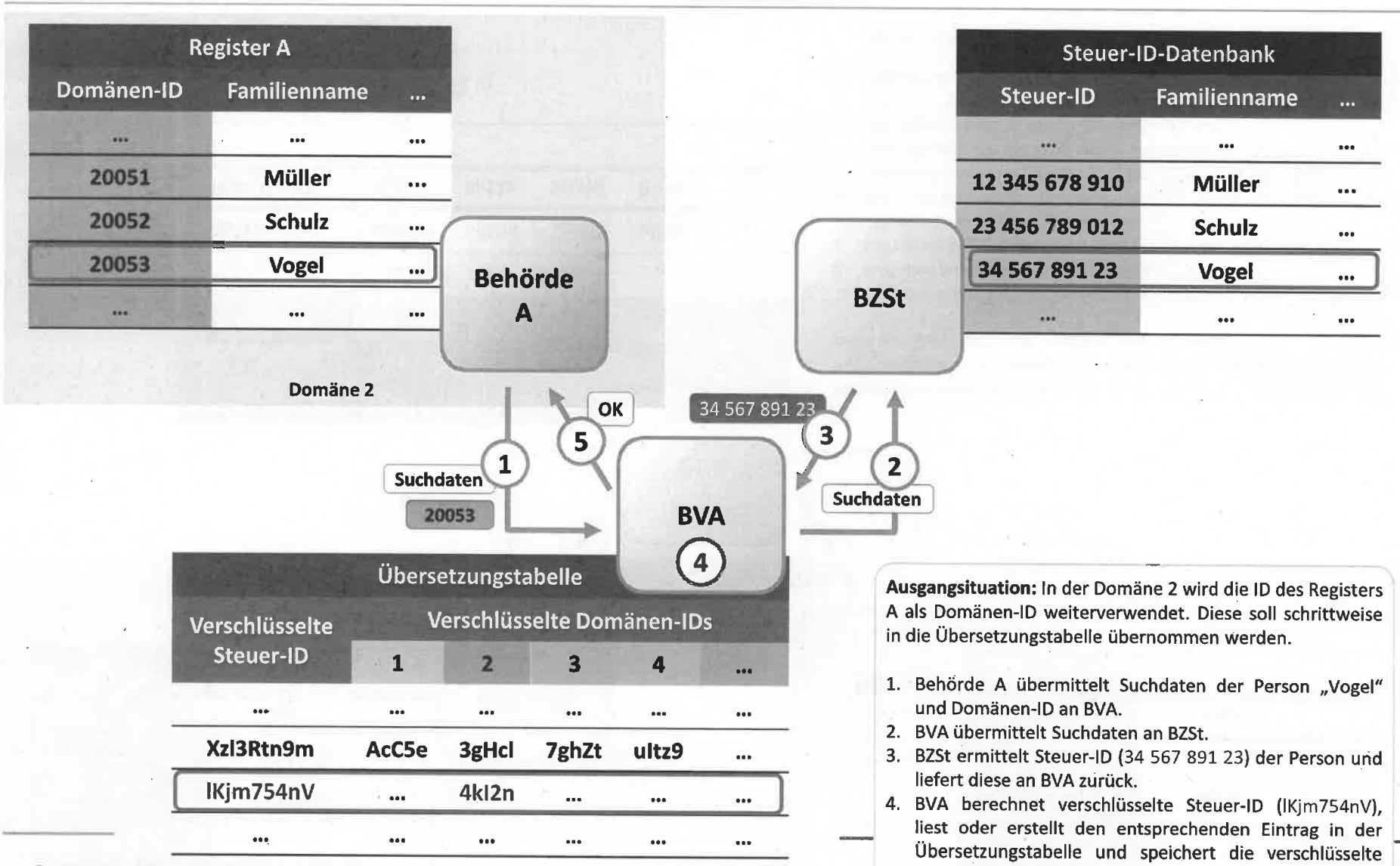
Das Domänen-ID-Modell maximiert den Datenschutz bei gleichzeitiger Minimierung des Aufwands.

- Durch die Aufteilung der Registerlandschaft in Domänen mit getrennten und verschlüsselten Domänen-IDs wird eine Profilbildung effektiv verhindert.
- Durch die Einführung einer gesicherten Übersetzungstabelle können Personen eindeutig in allen Domänen identifiziert werden, sofern dies rechtlich zulässig ist.
- Durch die maximale Wiederverwendung bestehender IDs wird der Anpassungsbedarf in den Registern minimiert.

➢ Die Lösung vereint die Vorteile des aktuellen Gesetzentwurfs mit denen des „österreichischen Modells“, ohne dessen Nachteile zu übernehmen.

Anhang mit Detaildarstellungen

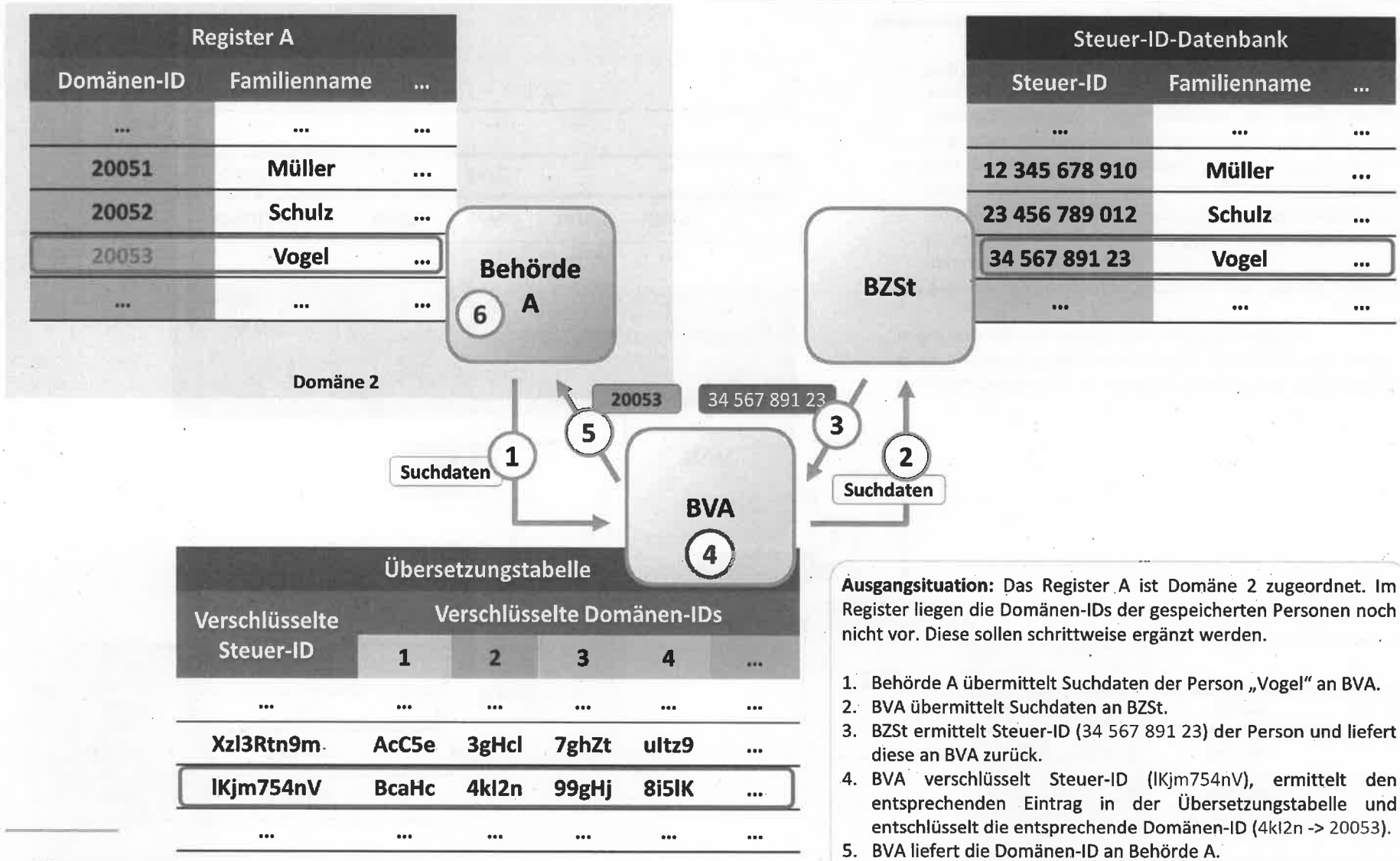
Szenario: Erstbefüllung der Übersetzungstabelle



Ausgangsituation: In der Domäne 2 wird die ID des Registers A als Domänen-ID weiterverwendet. Diese soll schrittweise in die Übersetzungstabelle übernommen werden.

1. Behörde A übermittelt Suchdaten der Person „Vogel" und Domänen-ID an BVA.
2. BVA übermittelt Suchdaten an BZSt.
3. BZSt ermittelt Steuer-ID (34 567 891 23) der Person und liefert diese an BVA zurück.
4. BVA berechnet verschlüsselte Steuer-ID (lKjm754nV), liest oder erstellt den entsprechenden Eintrag in der Übersetzungstabelle und speichert die verschlüsselte Domänen-ID (4kl2n).
5. BVA liefert Erfolgsmeldung an Behörde A.

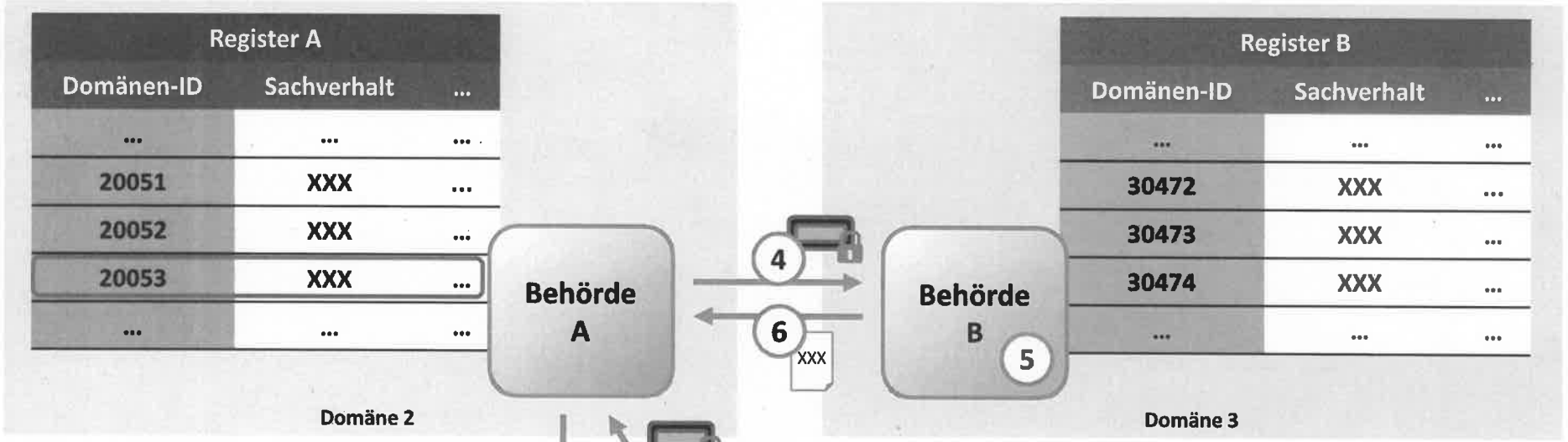
Szenario: Zuordnung einer vorhandenen Domänen-ID



Ausgangsituation: Das Register A ist Domäne 2 zugeordnet. Im Register liegen die Domänen-IDs der gespeicherten Personen noch nicht vor. Diese sollen schrittweise ergänzt werden.

1. Behörde A übermittelt Suchdaten der Person „Vogel" an BVA.
2. BVA übermittelt Suchdaten an BZSt.
3. BZSt ermittelt Steuer-ID (34 567 891 23) der Person und liefert diese an BVA zurück.
4. BVA verschlüsselt Steuer-ID (lKjm754nV), ermittelt den entsprechenden Eintrag in der Übersetzungstabelle und entschlüsselt die entsprechende Domänen-ID (4kl2n -> 20053).
5. BVA liefert die Domänen-ID an Behörde A.
6. Behörde A speichert die Domänen-ID zur Person „Vogel" in Register A.

Szenario: Domänenübergreifende Datenabfrage



Übersetzungstabelle					
Verschlüsselte Steuer-ID	Verschlüsselte Domänen-IDs				
	1	2	3	4	...
...	...	...	...	...	...
Xzl3Rtn9m	AcC5e	3gHcl	7ghZt	ultz9	...
lKjm754nV	BcaHc	4kl2n	99gHj	8i5lK	...
...	...	...	...	...	...

Ausgangsituation: Behörde A aus Domäne 2 benötigt die Sachverhalte einer Person aus Register B der Domäne 3. Die Domänen-ID der Person in der Domäne 2 liegt bereits vor.

1. Behörde A übermittelt Domänen-ID der Person (20053) an BVA.
2. BVA führt folgende Schritte durch
   - Kontrolle der Rechtmäßigkeit der Anfrage
   - Verschlüsselung die Domänen-ID (20053 -> 4kl2n)
   - Lesen des entsprechenden Eintrags aus der Übersetzungstabelle
   - Entschlüsselung der Domänen-ID 3 (99gHj -> 30474)
3. BVA verschlüsselt die Domänen-ID (30474) mit dem Schlüssel der Behörde B und liefert das Ergebnis an Behörde A zurück.
4. Behörde A ruft die Sachverhalte der Person bei Register B ab und übermittelt die verschlüsselte Domänen-ID.
5. Behörde B entschlüsselt die Domänen-ID und liest den entsprechenden Eintrag.
6. Behörde B liefert die gelesenen Sachverhalte an Behörde A.