

Confidential Relay Service (CRS)

Skizze einer Produktidee

Tobias Eisenhuth

October, 2025

Contents

1. Problem Space	2
1.1. Fire & Forget	2
1.2. Self-Service heute	2
2. Solution Space	3
2.1. Single Source of Truth	3
2.2. Einführung: Confidential Relay Service (CRS)	3
2.3. Herzstück	3
2.4. Use Case	5
2.5. Einschränkungen	5
2.6. Abgrenzungen – Der Confidential Relay Service	5
2.7. Externe Validierung	5
3. Strategie	5
3.1. Kano Grid	5
3.2. Monetarisierung	6
3.3. Preisfindung	6
3.4. Marketing	6

1. Problem Space

1.1. Fire & Forget

Im B2C-Kontext heißt „Daten teilen“ meist: Kundendaten werden initial und einmalig – etwa bei Kontoeröffnung oder Vertragsabschluss – beim jeweiligen Unternehmen hinterlegt. So entstehen verteilte und isolierte Kopien, deren Datenqualität aus Unternehmenssicht mit der Zeit sinkt. Wer als Kunde nicht dokumentiert, wann und welche Informationen mit welchem Unternehmen geteilt wurden, verliert schnell den Überblick. Das zeigt sich oft erst, wenn ein Geschäftsablauf aufgrund veralteter Daten scheitert – Unternehmen müssen dann auf alternative Quellen zurückgreifen oder aufwendig recherchieren. Seien es veraltete Rufnummern nach dem Anbieterwechsel, der Nachname, der sich durch Heirat ändert oder die Anschrift beim Umzug. In Deutschland ziehen jährlich immerhin ca. **8,4 Mio. Menschen** um – im Schnitt **23.000 pro Tag** [\[Umzugsstudie\]](#).

1.2. Self-Service heute

Die Deutsche Post erkennt und bedient den Bedarf an Adresspflege und Adressvermarktung mit einem eigenen Joint Venture mit Bertelsmann – der PostAdress.

“Die Deutsche Post Adress bietet Ihnen ganzheitliche Adressmanagement-Branchen-Lösungen, mit denen Sie den effizienten Kontakt zu Ihren Kunden sicherstellen. Mit uns überprüfen, korrigieren, aktualisieren, bereinigen und pflegen Sie Ihre Kundenadressen optimal.”

— [\[Webauftritt Deutsche Post 18.09.2025\]](#)

Die Datenbasis speist sich u. a. aus Einwohnermeldedaten, weiteren Datenbanken [\[PostAdress Webauftritt 18.09.2025\]](#), und aus Angaben von Postkunden im Rahmen des Nachsendeauftrags [\[Umzugsstudie\]](#). Das zeigt: Unternehmen haben ein starkes Interesse an aktuellen Kontaktdaten. Gleichzeitig sind Kunden bereit, aktiv an der Pflege mitzuwirken.

Mittlerweile haben Self-Service-Angebote zur Pflege von Stammdaten direkt in Portalen und Smartphone-Apps von Unternehmen Einzug gefunden. Beispiele:

Unternehmen	Produkt	Selbstverwaltete Attribute	Vermarktung
Deutsche Post	Nachsendeauftrag	Adresse	Ja
Lidl	Lidl-Plus-App	Adresse, Telefon, E-Mail	Nein
Sparkassen	Banking-App	Adresse, Telefon, E-Mail	Nein
Allianz	Webportal	Adresse, Bankverbindung	Nein
Allianz Direct	Webportal	Adresse, Telefon, E-Mail	Nein
ING Deutschland	Banking-App	Adresse, Telefon, E-Mail, Name (mit ID-Nachweis)	Nein

Pain Points

1. Als Kunde fehlt mir der Überblick über meine Geschäftsbeziehungen und die Auswirkungen veralteter Stammdaten.
2. Bei Änderungen müssen dieselben Informationen proaktiv an verschiedenen Stellen nachgepflegt werden.

2. Solution Space

2.1. Single Source of Truth

Die konzeptionelle Lösung liegt auf der Hand: eine zentrale Datenbank, die für Unternehmen als **Single Source of Truth** dient.

Innerhalb von Unternehmensnetzwerken ist ein solcher Ansatz etabliert. Bis dato gibt es jedoch keinen unternehmensübergreifenden Anbieter, der eine direkt an die IT-Infrastruktur angebundene Lösung bietet. Ursache sind weniger technische Hürden als vielmehr berechtigte Datenschutzbedenken. Damit ein solcher Dienst Akzeptanz bei Unternehmen und Kunden findet – und kommerziell erfolgreich sein kann – müssen folgende Eigenschaften erfüllt sein:

1) Privatsphäre und Sicherheit

a) Zero-Trust-Architektur

- Im Falle eines Datenlecks am Datenbankdienst werden keine personenbezogenen Daten preisgegeben.

2) Funktionalitäten

a) Übersicht über Geschäftsbeziehungen

- Welches Unternehmen (oder welche Organisation) hält welche Daten über mich?

b) Selbstverwaltung beliebiger personenbezogener Daten (von atomaren Informationen wie Telefonnummern bis hin zu Dokumenten wie Geburtsurkunden)

- Teilen
- Aktualisieren
- Löschen (inkl. Löschungsantrag an Empfänger)
- Berechtigungen verwalten

2.2. Einführung: Confidential Relay Service (CRS)

Der CRS ist ein Onlinedienst, der die obigen Anforderungen an Sicherheit und Privatsphäre basierend auf dem Konzept der Proxy-Re-Encryption technisch sicherstellt. Er ergänzt diese Basis um Self-Service-Funktionalitäten auf Grundlage einer Übersicht der Geschäftsbeziehungen. Dazu gehören eine Client-App für Nutzer sowie eine REST-Schnittstelle für Unternehmen. Im Folgenden liegt der Fokus auf dem technischen Kernkonzept, da dies die Grundlage für die Machbarkeit darstellt.

2.3. Herzstück

Die Proxy-Re-Encryption ermöglicht Ende-zu-Ende-Verschlüsselung, bei der ein bereits unter **key_pair_A** verschlüsseltes Geheimnis für einen Empfänger unter **key_pair_B** zugänglich gemacht werden kann. Die notwendige Transformation ergibt sich mittels des **transform_key_A2B**, welcher aus **private_key_A** und **public_key_B** erzeugt wird. Diese Transformation übernimmt – wie der Name suggeriert – ein Proxy.

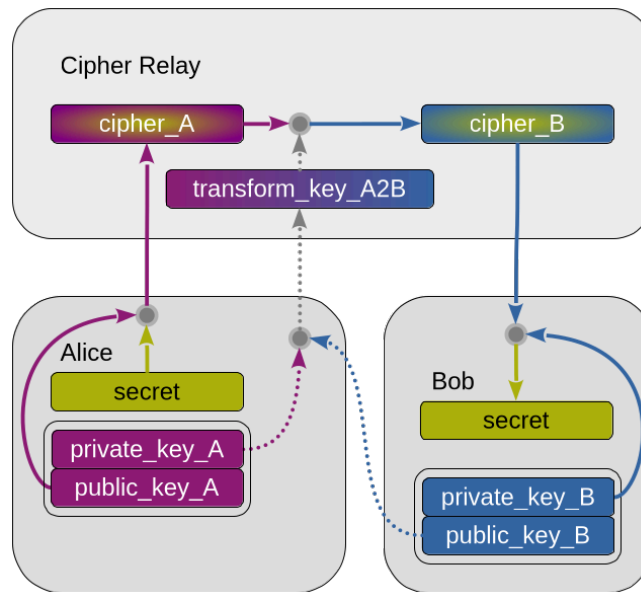


Figure 1: Re-Encryption-Schema zwischen Alice → Bob über einen Proxy („Cipher Relay“).

Garantie:

Das Geheimnis wird zu keinem Zeitpunkt gegenüber dem "Cipher Relay" offenbart. Die Privatsphäre des Nutzers ist damit gewährleistet.

Analog lassen sich auch **transform_key_A2C**, **transform_key_A2D** usw. erzeugen und beim „Cipher Relay“ hinterlegen.

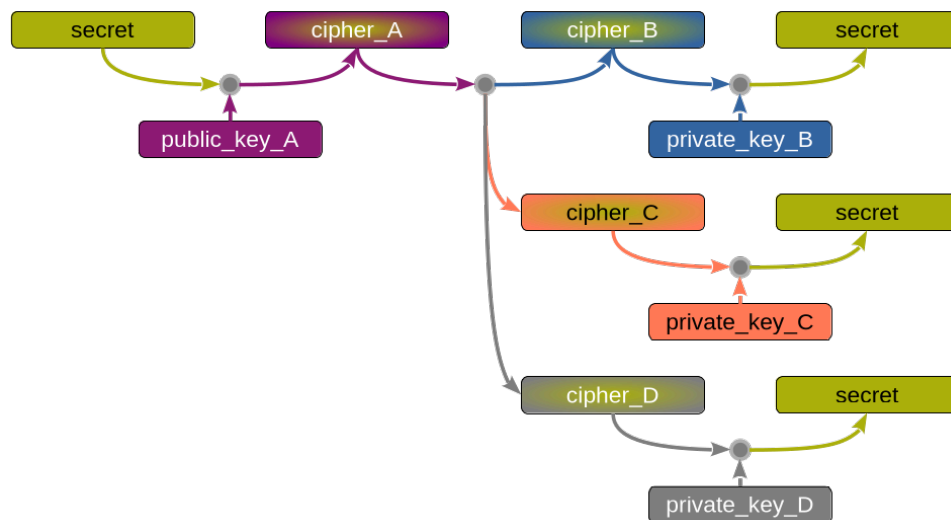


Figure 2: *cipher_A* lässt sich mit entsprechendem *transform_keyA2X* in *cipher_X* überführen.

Erkenntnisse:

1. Der "Cipher Relay"-Dienst muss nur *cipher_A* und die entsprechenden Transform-Keys halten, um seine Aufgabe zu erfüllen.
2. Eine Aktualisierung von *cipher_A* (inkl. neuem Nonce) kann ohne Neuverhandlung der Schlüssel propagiert werden.
3. Das Löschen eines *transform_key_A2X* beendet die Beziehung zu Partei_X endgültig.

2.4. Use Case

Ein Nutzer möchte online oder vor Ort ein Konto bei einer Bank eröffnen. Der angestammte Geschäftsprozess unterscheidet sich zunächst nicht, bis es zum Austausch personenbezogener Daten kommt. Dieser Schritt findet digital statt – entweder online (z. B. via App und API) oder in der Filiale (z. B. via QR-Code und Scanner). Die Bank stellt über den CRS-Dienst eine Anfrage nach bestimmten personenbezogenen Daten. Der Nutzer bestätigt den Zugriff auf die angefragten Felder, ergänzt ggf. Informationen, die noch nicht im CRS hinterlegt sind, und hinterlegt eine Berechtigungsstrategie – einmaliges Teilen oder Weiterleiten von Aktualisierungen. Anschließend erfolgt die notwendige Kommunikation und Schlüsselgenerierung. Die Identitätskontrolle ist ausdrücklich kein Feature des Dienstes und muss wie gehabt durch die Bank erfolgen.

Aktualisiert ein Nutzer später seine Daten, so werden diese bei entsprechender Berechtigung an die Bank weitergeleitet.

2.5. Einschränkungen

Weitere notwendige Kunstgriffe, die solch einen Dienst erst möglich machen, z. B. das Mischen von symmetrischen und asymmetrischen Verschlüsselungsverfahren zur Effizienzsteigerung, sind hier bewusst ausgespart.

Ein weiterer Aspekt ist der Speicheroverhead der Schlüssel, der die ursprüngliche Datenmenge nicht unerheblich vergrößern kann (schlussendlich auch eine Frage der verwendeten Algorithmen). Hier sind verschiedene Wege gangbar, je nach Abwägung von technisch garantiertem und systematisch garantiertem Datenschutz.

2.6. Abgrenzungen – Der Confidential Relay Service

1. ist kein Data Broker – es werden weder Nutzerprofile erstellt noch vermarktet.
2. ist kein Identity Service wie VerifyMe oder die AusweisApp.
3. ist nicht als Löschungsdienst wie Incogni oder DeleteMe gedacht.
4. ist nicht als Backupserver für vertrauliche Dokumente ausgelegt.

2.7. Externe Validierung

Eine Blaupause für den Confidential Relay Service findet sich in einer Arbeit von *Hannes Zach et al.*: **“Using Proxy Re-Encryption for Secure Data Management in an Ambient Assisted Living Application”** [\[paper Hannes Zach et al.\]](#). Die Arbeit beschreibt einen analogen Anwendungsfall mit ähnlicher technischer Konzeption und Argumentation.

3. Strategie

3.1. Kano Grid

Kategorie	Attribut	Meldeamt	PostAdress	Acxiom	CRS
Must-have	Sicherheit	Mittel	Mittel	Mittel	Hoch
Performance	Datenart	Meldedaten	Adressdaten	Adress- & Verhaltensdaten	beliebige Daten
Performance	Geschäftsfeld	Rechtssachen	Marketing	Marketing	Datenpflege
Performance	Datenqualität	Hoch	Hoch	Hoch	Hoch
Delighter	Transparenz	Niedrig	Niedrig	-	Hoch
Delighter	Datenhoheit	-	Niedrig	-	Hoch

3.2. Monetarisierung

Da der Marktwert des CRS auf der Kooperation der Nutzer basiert, sind die Kernfunktionalitäten für diese kostenlos. Unternehmen zahlen einen monatlichen Betrag, abhängig von der Anzahl der abonnierten Nutzerdaten – also proportional zum kontinuierlichen Wert, den der Dienst bietet.

Auch auf Nutzerseite ist eine Monetarisierung nach dem Freemium-Modell denkbar, z. B. für erweiterten Speicher oder Peer-to-Peer-Dienste. Beispiel: Ein Nutzer möchte seine Mobilfunknummer privat mit Freunden teilen. Für den Sender ist dieser Dienst kostenpflichtig, für den Empfänger bleibt er kostenlos.

free resource packs

3.3. Preisfindung

Zur Einordnung:

- Die Deutsche Post erhebt für die Anmeldung eines Nachsendeauftrags 31,90 Euro von Privatpersonen.
- “Jede Umzugsadresse aus einem Nachsendeauftrag, bei dem der Nutzer der Weitergabe seiner Adresse nicht widersprochen hat, wird schätzungsweise bis zu zehn Mal zu jeweils 1,20 Euro aktualisiert.” [\[Wikipedia Artikel 18.09.2025\]](#)

Diese Zahlen dienen ausschließlich als Referenz und lassen keine Rückschlüsse auf die tatsächliche Preisgestaltung des CRS zu. Die Preisgestaltung kann derzeit nicht belastbar abgeleitet werden.

3.4. Marketing

Der Markteintritt erfolgt stufenweise:

1. Aufbau des CRS als Self-Service für die Verwaltung von Kundenstammdaten, zunächst für den eigenen Kundenstamm (z. B. Lidl- und Kaufland-Kunden im Rahmen einer Zusammenarbeit mit STACKIT).
2. Ausweitung auf ausgewählte Geschäftskunden von STACKIT sowie deren Kundenstämme.
3. Kommerzialisierung und Skalierung auf den breiteren Markt.

STACKIT fungiert dabei als strategischer Türöffner: Über die bestehende Konzernverankerung kann der CRS frühzeitig in realen Geschäftsumgebungen erprobt, validiert und an den Bedarf von Unternehmen angepasst werden.

In der ersten Phase liegt der Fokus auf der Gewinnung privater Nutzer und damit auf der Erhöhung des Marktpotenzials. Leicht verzögert erfolgt die Vermarktung an Unternehmen, die sich am aktuellen Marktwert orientiert – dieser wächst proportional zur steigenden Nutzerzahl des Self-Service.

Ein zentrales Prinzip ist, dass sich der Dienst nahtlos in die Prozesse der Unternehmen einfügt und dabei die Komplexität der zugrunde liegenden Kryptographie vollständig abstrahiert. Dadurch wird die Lösung für Unternehmen einfach integrierbar und ohne tiefes Spezialwissen nutzbar.