Confidential Relay Service - CRS
Skizze einer Produktidee

Tobias Eisenhuth
September, 2025

Contents

1. Problem Space

1.1. Fire & Forget

Im B2C-Kontext heißt „Daten teilen“ meist: Kundeninnenstammdaten werden initial und einmalig, z.B. bei Kontoeröffnung oder Vertragsabschluss, beim jeweiligen Unternehmen hinterlegt. So entstehen verteilte Kopien, deren Datenqualität aus Unternehmenssicht mit der Zeit sinkt. Wer als Kunden nicht dokumentiert, wann und welche Informationen mit welchem Unternehmen geteilt wurden, verliert schnell den Überblick. Das fällt spätestens dann auf, wenn sich doch etwas ändert: die Rufnummer nach Anbieterwechsel, der Nachname durch Heirat oder die Wohnanschrift beim Umzug. In Deutschland ziehen **jährlich** immerhin ca. **8,4 Mio. Menschen** um. Im Schnitt **23.000 pro Tag** [1].

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 Seinen Kunden sicherstellen. Mit uns überprüfen, korrigieren, aktualisieren, bereinigen und pflegen Sie Seine Kundenadressen optimal.”
>
> — Webauftritt Deutsch Post [2]

Die Datenbasis speist sich u. a. aus Einwohnermeldedaten, weiteren Datenbanken [3], und aus Angaben von PostKunden selbst, im Rahmen des Nachsendeauftrags [1]. Das zeigt: Unternehmen haben ein Interesse an integren 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 Unternhemen einzug gefunden. Beispielsweise:

Unternehmen	Produkt	Selbstverwaltete Attribute	Vermarktung
Deutsche Post	Nachsendeauftrag	Adresse	Ja
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 Point
1. Als Kunden, fehlt mir der Überblick über meine Geschäftsbeziehungen um die Auswirkungen meiner veralteten Stammdaten zu verstehen.
2. Als Kunden, muss ich bei Veränderung, proaktiv an verschiedenen Stellen die selbe Information nachpflegen.

2. Solution Space

2.1. Single Source of Truth

Die konzeptionelle Lösung ist offenichtlich – eine zentrale Datenbank, die für Unternehmen als single source of Truth dient.

Innerhalb unternehmensweiter netzwerkübergreifender Applikationen gang und gäbe, existiert bis dato kein unternehmenübergreifender Anbieter einer direkt an die IT-Infrastruktur von Unternehmen angebundene Lösung. Das liegt wohl weniger an Fragen der technischen Umsetzungs, sondern eher an berechtigten Bedenken an den Datenschutz. Damit ein solcher Dienst für Unternehmen und Kunden gleichermaßen überhaupt Akzeptanz findet, und damit kommerziell Erfolgreich sein kann, müssen aus meiner Sicht folgende Eigenschaften gegeben sein:

1) **Privatsphäre und Sicherheit**
   a) Zero Trust Architektur
      - Die Datenbank könnte prinzipiell öffentlich zugänglich sein ohne dabei geheime Daten preiszugeben.
2) **Feature**
   a) Übersicht über Geschäftsbeziehungen bieten
      - Wer hält welche Daten über mich?
   b) Selbstverwatlung beliebiger personenbezogener Daten (atomare Informationen wie Telefonnummer, als auch ganze Dateien wie Geburtsurkunden)
      - Teilen
      - Aktualisieren
      - Löschen und Löschungsantrag an Empfänger stellen
      - Berechtigungen verwalten
   c)

2.2. Enter Confidential Relay Service (CRS)

Ein online Dienst, der die obigen Anforderungen an Sicherheit und Privatsphäre basierend auf dem Konzept des Proxy-Re-Encryption technisch sicherstellt, und die Funktionalitäten des Self-Service auf

Basis einer Übersicht der Geschäftsbeziehungen. Dazu eine Client-App für Kunden, und eine REST-Schnittschelle für Unternhemen. Der Fokus liegt im folgenden ausschließlich auf das technischen Kernkonzept, da dies die Grundlage für die Machbarkeit darstellt.

2.3. Pièce de résistance

Die Idee hinter der Proxy-Re-Encryption ist eine Ende zu Ende Verschlüsselung zu realisieren, bei der ein bereits unter key_pair_A verschlüsseltes Geheimnis, einem Empfänger unter key_pair_B offenbart werden kann. Die dafür notwendige Transformation von einer Verschlüsselung in die Andere ergibt sich mittels des transform_key_A2B. Dieser wird aus private_key_A und public_key_B erstellt. Wie der Name suggeriert, übernimmt die Transformation, im standard Schema, ein Proxy. – *Figure 1*

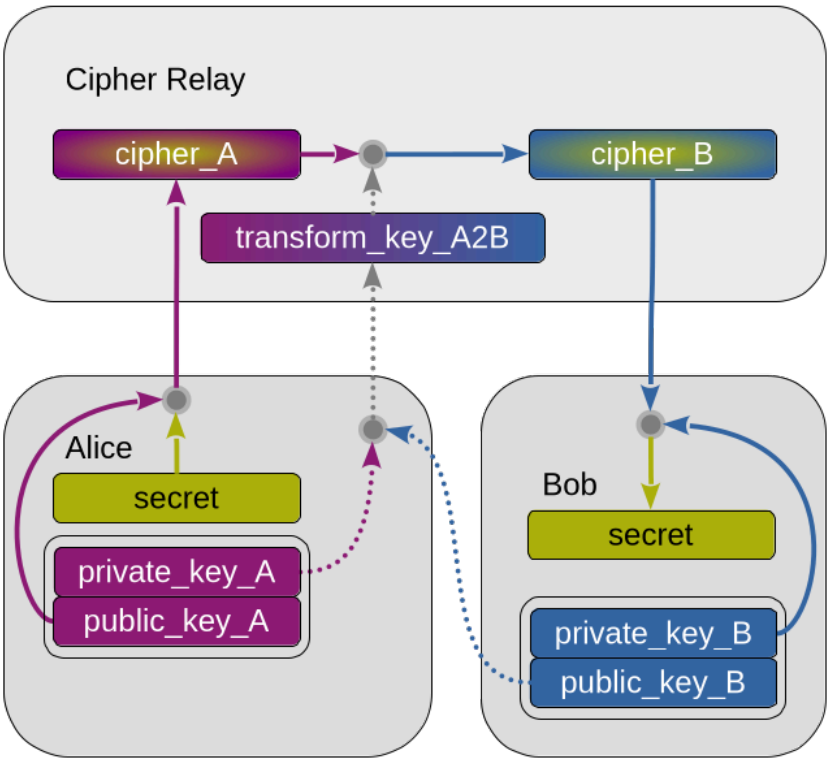

Figure 1: Re-encryption Schema zwischen Alice -> Bob, über einen Proxy “Cipher Relay”.

Garantie:
Das Gehemnis wir zu keinem Zeitpunkt gegebüber dem "Cipher Relay" offenbart. Der Schutz und die Privatsphäre an den personenbezogenen Daten der Nutzerinnen ist damit gewährleistet.

Auf gleiche Weise lässt sich auch ein transform_key_A2C, transform_key_A2D, usw. erstellen und beim “Cipher Relay” hinterlegen.

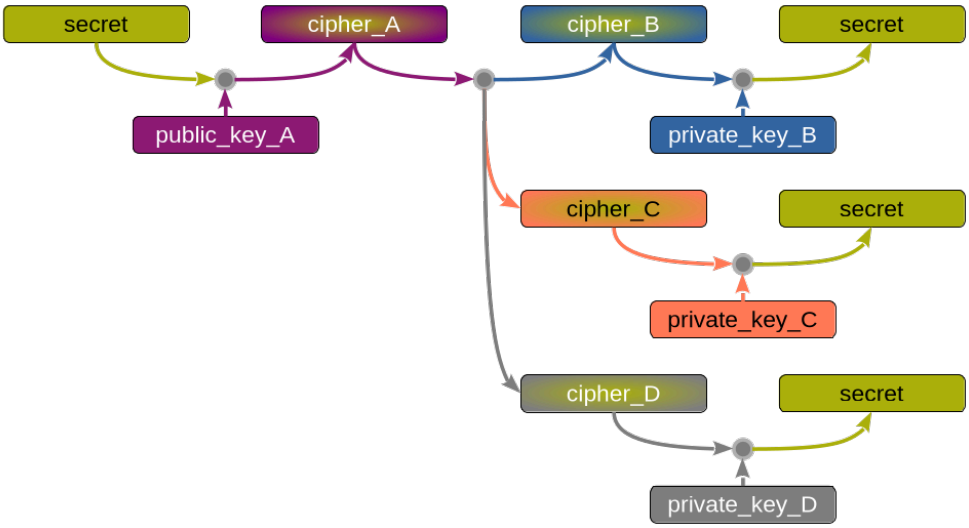

Figure 2: *cipher_A* lässt sich mit entsprechendem *transform_keyA2X* in *cipher_X*.

Erkenntnis:
1. Der "Cipher Relay" Dienst, muss nur den ciper_A und die entsprechenden transform keys halten, um seine Aufgabe wahr nehmen zu können.
1.2 Eine Aktualisierung von cipher_A (inkl. neuem nonce) lässt sich ohne Neuverhandeln der Schlüssel weiterproagieren. (trivial)
3. Löschen des transform_key_A2X kappt das Verhältnis zu Partei_X endgültig.

2.4. Use case

Eine Kunden möchte online oder vorort ein Konto bei einer Bank eröffnen. Der Geschäftsprozess unterscheidet sich erstmal nicht, bis es zum Austasch der personenbezogenen Daten kommt. Dieser Schritt findet digital, entweder online oder z.B. in einee Smartphone App und unernehmsseitig einer API statt. Die Bank, sendet eine entsprechende Anfrage über den CRS-Dienst an die Kunden, mit dem Ersuchen nach einem bestimmten Satz personenbezogener Daten. Die Kundnin bestätigt den Zugriff auf die angefragten Felder und ergänzt ggf. Infromationen die noch nicht im CRS hinterlegt wurden. Im nächten Schritt findet die notwendige Kommunikation (Verschlüsselter online Kanal, oder persönlich in der Filiale z.B. QR-code und Scanner) und Generierung der Schlüssel statt. Die Identitäskontrolle ist ausdrücklich kein Feature des Dienstes, und muss wie gehabt erfolgen.

2.5. Caveat

Die weiter notwendigen Kunstgriffe, die solch einen Dienst erst möglichen machen, sind hier für den gorben Abriss zunächst unterschlagen. Themen wie das Mischen von symetrischen und asymetrischen Verschlüsselungsverfahren zur Effizientzsteigerung z.B.

Oder der Speicheroverhead der Schlüssel, der die ursprüngliche Datenmenge nicht unerheblich aufbläht (Schlussendlich auch eine Frage der verwendeten Algorithmen). Besonders für kleine atomare Informationen wie die Hausnummer ist das Verhältnis von Daten zu Overhead ungünstig, wenn auch absolut doch im Rahmen. Hier stellt sich die Frage wie feingranular die technische Gewährleistung des Schutzes der Daten gehen soll. Z.B. könnten auch mehrere Informationen unter einem transform_key in einem Paket zusammengefasst werden, und die feingranulare Verteilung vertrauensvoll durch den CRS, über Berechtigungen geregelt sein. Im Falle eines Lecks beim CRS, würden gegenüber einem Unternehmen, dass nur Berechtigungen für einen Teil eines Pakets inne hat, potenziell die gesammten Daten dieses Pakets offenbart.

2.6. Abgrenzungen - Der Confidential Relay Service

1. ist kein Databroker - weder werden Nutzerprofile erstellt noch vermarktet.
2. ist kein Löschungsdienst wie Incogni oder DeletMe.
3. ist kein Identityservice wie VerifyMe, oder die AusweisApp.
4. ist kein Backupserver für vertraulische Dokumente.

2.7. Fun Fact

Eine Blaupause für den Confidential Relay Service findet sich in wieder in einer Arbeit von *Hannes Zach et al.* "Using Proxy Re-Encryption for Secure Data Management in an Ambient Assisted Living Application" [4], das jüngst im Zuge eigener Recherchen , Es beschreibt einen analogen Anwendungsfall mit einigen Paralellen in der technischen Konzeption, und ähnliche Argumenten.

3. Strategie

3.1. Kano Grid

Kathegorie	**Attribut**	**Meldeamt**	**PostAdress**	**Acxionm**	**CRS**
must have	Sicherheit	Mittel	Mittel	Mittel	Hoch
performance	Datenart	Meldedaten	Adressdaten	Adressdaten & Verhaltensdaten	beliebige Daten
performance	Geschäftsfeld	Rechtssachen	Marketing	Marketing	Datenpflege
performance	Datenqualität	Hoch	Hoch	Hoch	Hoch
delighter	Transparenz	Niedrig	Niedrig	-	Hoch
delighter	Datenhoheit	-	Niedrig	-	Hoch

4. Monitarisierung

Da der Marktwert des CRS auf einen Kundenstamm angewiesen ist, sind die fundamentalen Grundfunktionalitäten für Kunden frei. Unternehmen zahlen einen monatlichen Betrag der von der Anzahl an Abonnierten Daten abhängig ist. Also proportional zum Nutzen, und wiederkehrend.

Kundenseitig ist ebenfalls ein Freemium denkbar für erweiterten Speicher oder peer to peer Dienste. Z.B. möchte eine Kunden seine Mobilfunknummer im privaten an andere Nutzer im Freundeskreis teilen, so ist das für den Sender kostenpflichtig und für den Empfänger weiterhin kostenlos.

5. Marketing

Aufbau des Dienstes als Self-Service für eigenen Kundenstamm, aufweiten auf Kundenstamm von Partner und schließlich voll Kommerzialisieren. Dabei zunächst Fokus auf Kunden-Marktanteil, und späterer gradueller Anpassung der Monitarisierung durch Unternehmen an den Marktwert durch Kundenstamm.