Aufgabe Schuldenfroh

Als Teil ihrer Strategie zur Verbesserung des Dokumentations-Workflows bittet die Kreditkartenfirma “Schuldenfroh” um ein redesign ihrer Datenbank. Nachdem Sie sich vergewissert haben, dass die Beschreibung wenigstens ein paar Anglizismen enthält, machen Sie sich an die Arbeit.

Jede Kreditkarte ist eindeutig identifiziert durch ihre Kartennummer (KNR). Zusätzlich muss das Ablaufdatum (ABLAUFDATUM) und der Sicherheitscode (CVC) vermerkt sein. Ersetzt eine Karte eine ältere Karte, so wird gespeichert welche Karte ersetzt wird (jede Karte kann maximal eine andere Karte ersetzen und durch maximal eine andere Karte ersetzt werden), und ab wann die neue Karte gültig ist (AB).

KundInnen haben eine eindeutige Kundennummer (KNR). Zusätzlich ist ihr Vor- und Nachname (VNAME, NNAME) und ihr Geburtsdatum (GEBDAT) bekannt, wobei die Kombination aus Vorname, Nachname und Geburtsdatum ebenfalls eindeutig ist. Außerdem muss für jede Kundin/jeden Kunden eine Kontonummer (IBAN) vorhanden sein.

Bei Kreditkarten wird unterschieden auf welche Kundin/welchen Kunden die Kreditkartet lautet auf der einen, und welche KundInnen für eine Karte zeichnungsberechtigt sind auf der anderen Seite. Jede Kreditkarte lautet auf genau eine Kundin/einen Kunden. Jede Kundin/Jeder Kunde kann jedoch für beliebig viele Karten zeichnungsberechtigt sein, wobei für jede Karte die Anzahl der Zeichnungsberechtigten auf 5 begrenzt ist.

Partner der Kreditkartenfirma sind sowohl durch ihren Markennamen (MNAME) eindeutig identifiziert, als auch durch ihre Partner-ID (PID). Bei Partnern wird zwischen Vertriebspartnern und Bezahlpartnern unterschieden. Vertriebspartner vergeben Kreditkarten, wobei jede Karte von genau einem Vertriebspartner vergeben werden muss. Für Vertriebspartner wird neben dem Preis (PREIS) einer Karte auch der Prozentsatz (ANTEIL) gespeichert, den der Vertriebspartner von jedem mit der Karte getätigten Umsatz erhält. Bezahlpartner sind Unternehmen welche Kreditkarten von “Schuldenfroh” akzeptieren. Für jeden Bezahlpartner wird der Anteil des Umsatzes gespeichert der als Gebühr abgeführt werden muss (GEBUEHR). Manche Vertriebspartner gewähren einen Rabatt bei Zahlungen mit bestimmten Bezahlpartnern. Es soll vermerkt werden, welcher Vertriebspartner bei welchem Bezahlpartner welchen Rabatt (PROZENT) gewährt.

Jeder Bezahlpartner erhält mindestens einen Account. Ein Account ist eindeutig identifiziert durch den Bezahlpartner sowie durch den Benutzernamen (BENUTZER). Zusätzlich soll für jeden Account das Passwort (PW), sowie sämtliche Loginversuche gespeichert werden. Ein Login(versuch) wird eindeutig identifiziert durch den Account, sowie durch das Datum (DATUM) des Logins, gemeinsam mit einer id (ID). Darüber hinaus wird die IP-Adresse des Logins gespeichert (IP), und ob der Login erfolgreich war (SUCCESS). MitarbeiterInnen von Bezahlpartnern werden durch ihre Sozialversicherungsnummer (SNVR) eindeutig identifiziert. Darüber hinaus wird ihr Vorname (VNAME), Nachname (NNAME), ihr Geburtsdatum (GEBDAT), sowie ihr Gehalt (GEHALT) gespeichert. Es wird nicht gespeichert, welche MitarbeiterInnen bei welchem Partner arbeiten, sondern nur, welche MitarbeiterInnen Zugriff auf welchen Account haben, wobei es für jeden Account mindestens eineN MitarbeiterIn mit Zugriff geben muss.

Eine Transaktion ist eindeutig identifiziert durch die Kreditkarte auf welche sie gebucht wurde, den Account mit dem die Buchung durchgeführt wurde, sowie durch eine Transaktionsid (TID). Zu jeder Transaktion wird außerdem der Betrag (TOTAL) sowie das Datum (DATUM) gespeichert.

Jedes Security-Level ist eindeutig bezeichnet durch seinen Namen (NAME) in Kombination mit seiner Nummer (NR). Für jede Transaktion wird genau ein Security-Level verwendet. Die Kreditkartenfirma beschäftigt Security-Agents. Zu jedem Security-Agent wird ein Name (NAME), sein Trust-Level (TLEVEL), sowie eine eindeutige Agent-ID (AID) verwaltet. Zu Transaktionen, bei denen der Verdacht auf einen Betrugsfall besteht wird zusätzlich noch eine Bemerkung (BEM), die Art des Betrugs (TYP), das Datum an dem der Betrugsverdacht erkannt wurde (DATUM) gespeichert, sowie welcher Security-Agent den Verdacht gemeldet hat. Sobald einE KundeIn auf einen Verdachtsfall reagiert wird das Datum (DATUM) der Reaktion gespeichert, sowie ob es sich in der Tat um einen Betrug handelt oder nicht (OK).

Es soll weiter gespeichert werden, welcher Security-Agent welcheN MitarbeiterIn zu welchem Security-Level zugelassen hat, und wann das passiert ist (AM). Es gilt zu beachten, dass jedeR MitarbeiterIn zu mindestens einem Security-Level zugelassen sein muss.