Z-Spezifikation für FINMA-Rundschreiben (CIDOperationelle Risiken - Banken, Schweiz)
Entwickelt von Serge (Siarhei Vinahradau, vinahradau@yahoo.de)
Sprache: Z

Rundschreiben, Anhang 3, Umgang mit elektronischen Kundendaten (weiterhin als FINMA bezeichnet):
https://www.finma.ch/de/~/media/finma/dokumente/rundschreiben-archiv/finma-rs200821---30-06-2017.pdf

Anforderungen des Rundscreibens:
- Klassifikation der Kundendaten, oder CID (FINMA 10*)
    DATENKATEGORIE
    CIDDATENKATEGORIEN
    METADATEN
- Für CID verantwortliche Einheiten (FINMA 13*)
    EINHEIT
    BANK
- Die Bank muss wissen, wo CID gespeichert wird (FINMA 15*)
    CIDSYSTEMEINVENTAR
- Länder: erhöhte Risiken der CID-Speicheerung ausserhalb der Schweiz (FINMA 20*)
    LAND
- Systeme für Speicherung und Zugriff ausserhalb der Schweiz haben ihre CIDs gesschützt (anonymiziert, pseudoanonymisiert, verschlüsselt) (FINMA 20*)
  INHALT
  DatenSpeichern
- Ein rollen- und funktionsspezifisches Autorosoerungssystem regelt CID-Zugriffsberechtigungen (FINMA 22*)
    ROLLE
    CIDROLLEN
    BENUTZER
    BANK
- Liste der Benutzer mit Zugriff auf Massen-CID (FINMA 34*)
    MassenCIDZugriffsberechtigungListe
- Datenbearbeitung mit Massen-CIDs: Log-Dateien (FINMA 40*)
    CIDMASSENZUGRIFFSLOG
- Interne Mitarbeitende, verantwortlich für ausgelagerte CID-Aktivität (FINMA 50*)
    BANK
    BENUTZER
    BenutzerHinzufuegen
    InternenBenutzerHinzufuegen
    ExternenBenutzerHinzufuegen

```
_
  DATENKATEGORIE ::= DIREKT | INDIREKT | POTENZIELLINDIREKT | GESCHUETZT | NICHTCID
  CIDDATENKATEGORIEN == {DIREKT, INDIREKT, POTENZIELLINDIREKT}
  LAND ::= SCHWEIZ | GROSSBRITANNIEN | USA | DEUTSCHLAND
  METADATEN ::= KUNDENNAME | KUNDENADRESSE | PROMINENZSTATUS
  INHALT ::= MUSTERMANN | SEESTRASSE | JA | NEIN | XXXXX
  EINHEIT ::= EINHEIT1 | EINHEIT2 | EINHEIT3
  BENUTZER ::= BENUTZER1 | BENUTZER2 | BENUTZER3
  ROLLE ::= ROLLEGUIBENUTZERCID | ROLLEGUIBENUTZER | ROLLEMASSENZUGRIFFCID |
ROLLEMASSENZUGRIFFNICHTCID | ROLLE1
  CIDROLLEN == {ROLLEGUIBENUTZERCID , ROLLEMASSENZUGRIFFCID}
  SYSTEMID ::= SYSTEM1 | SYSTEM2 | SYSTEM3
L
```

```
┌ SYSTEM
  SystemId: SYSTEMID
  SystemLand: LAND
  SystemDatenklassifizierung: METADATEN ⇸ DATENKATEGORIE
  SystemDateninhalte: METADATEN ⇸ INHALT
  SystemMetadaten: ℙ METADATEN
  SystemInhalteMetadaten: ℙ METADATEN
|
  SystemLand = SCHWEIZ ∨ (∀ c : ran SystemDatenklassifizierung • c ∉ CIDDATENKATEGORIEN)
  dom SystemDateninhalte ⊆ dom SystemDatenklassifizierung
  SystemMetadaten = dom SystemDatenklassifizierung
  SystemInhalteMetadaten = dom SystemDateninhalte
└

┌ CIDSYSTEMEINVENTAR
  SYSTEM
  CIDSpeichersystemeIds: ℙ SYSTEMID
|
   ∀ Datenkategorie : ran SystemDatenklassifizierung • Datenkategorie ∈
CIDDATENKATEGORIEN ⇒ SystemId ∈ CIDSpeichersystemeIds
└
```

┌ BANK
  Datenklassifizierung: METADATEN ⇸ DATENKATEGORIE
  VerantwortlicheEinheiten: METADATEN ⇸ EINHEIT
  Rollen: ROLLE ↔ METADATEN
  Teams: EINHEIT ↔ BENUTZER
  InterneBenutzer: ℙ BENUTZER
  ExterneBenutzer: ℙ BENUTZER
  BenutzerZugriffsrechte: BENUTZER ↔ ROLLE

  KlassifizierungMetadaten: ℙ METADATEN
  VerantwortlicheMetadaten: ℙ METADATEN
  RollenRollen: ℙ ROLLE
  TeamsTeams: ℙ EINHEIT
│

  ∀ u : BENUTZER • ¬(u ∈ InterneBenutzer ∧ u ∈ ExterneBenutzer)
  ∀ u : dom BenutzerZugriffsrechte • u ∈ ran Teams
  ∀ u : dom BenutzerZugriffsrechte • u ∈ InterneBenutzer ∨ u ∈ ExterneBenutzer
  ∀ u : ExterneBenutzer • ¬(BenutzerZugriffsrechte⦇{u}⦈ ∩ CIDROLLEN ≠ ∅ ∧ Teams⦇dom
(Teams ▷ {u})⦈ ∩ InterneBenutzer = ∅)

  KlassifizierungMetadaten = dom Datenklassifizierung
  VerantwortlicheMetadaten = dom VerantwortlicheEinheiten
  RollenRollen = dom Rollen
  TeamsTeams = dom Teams
  dom Datenklassifizierung ⊆ dom VerantwortlicheEinheiten
└

┌ CIDMASSENZUGRIFFSLOG
  CIDMassenzugriffslog: BENUTZER ↔ SYSTEMID
└

┌ BankInitiieren
  BANK ′
  SYSTEM ′
  CIDSYSTEMEINVENTAR ′
  CIDMASSENZUGRIFFSLOG ′
│
  VerantwortlicheMetadaten′ = ∅
  KlassifizierungMetadaten′ = ∅
  Teams′ = ∅
  InterneBenutzer′ = ∅
  ExterneBenutzer′ = ∅
  BenutzerZugriffsrechte′ = ∅
  SystemMetadaten′ = ∅
  CIDSpeichersystemeIds′ = ∅
  SystemId′ = SYSTEM1
  CIDMassenzugriffslog′ = ∅
└

┌ DatenverantwortungZuordnen
  ΔBANK
  MetadatenEingabe?: METADATEN
  EinheitEingabe?: EINHEIT
|
  VerantwortlicheEinheiten′ = VerantwortlicheEinheiten ⊕ {MetadatenEingabe? ↦
EinheitEingabe?}
  Rollen′ = Rollen
  BenutzerZugriffsrechte′ = BenutzerZugriffsrechte
  Teams′ = Teams
  InterneBenutzer′ = InterneBenutzer
  ExterneBenutzer′ = ExterneBenutzer
└

┌ DatenKlassifizieren
  ΔBANK
  MetadatenEingabe?: METADATEN
  DatenkategorieEingabe?: DATENKATEGORIE
|
  Datenklassifizierung′ = Datenklassifizierung ⊕ {MetadatenEingabe? ↦
DatenkategorieEingabe?}
  Rollen′ = Rollen
  BenutzerZugriffsrechte′ = BenutzerZugriffsrechte
  Teams′ = Teams
  InterneBenutzer′ = InterneBenutzer
  ExterneBenutzer′ = ExterneBenutzer
└

─
  DatenklassifizierungImplementieren == DatenverantwortungZuordnen ∧ DatenKlassifizieren
└

┌ DatenRecyclen
  ΔBANK
  MetadatenEingabe?: METADATEN
|
  MetadatenEingabe? ∈ VerantwortlicheMetadaten
  MetadatenEingabe? ∈ KlassifizierungMetadaten
  Datenklassifizierung′ = {MetadatenEingabe?} ⩤ Datenklassifizierung
  VerantwortlicheEinheiten′ = {MetadatenEingabe?} ⩤ VerantwortlicheEinheiten
  Rollen′ = Rollen
  BenutzerZugriffsrechte′ = BenutzerZugriffsrechte
  Teams′ = Teams
  InterneBenutzer′ = InterneBenutzer
  ExterneBenutzer′ = ExterneBenutzer
└

┌ DatenSpeichern
ΔSYSTEM
ΔCIDSYSTEMEINVENTAR
ΞBANK
SystemIdEingabe?: SYSTEMID
SystemLandEingabe?: LAND
SystemMetadatenEingabe?: METADATEN
SystemDateninhaltEingabe?: INHALT
│
SystemLand′ = SystemLandEingabe?
∧ SystemId′ = SystemIdEingabe?
∧
(
(SystemLandEingabe? = SCHWEIZ ∧ (Datenklassifizierung SystemMetadatenEingabe?) ∈ CIDDATENKATEGORIEN
∧ CIDSpeichersystemeIds′ = CIDSpeichersystemeIds ∪ {SystemIdEingabe?}
∧ SystemDateninhalte′ = SystemDateninhalte ⊕ {SystemMetadatenEingabe? ↦ SystemDateninhaltEingabe?}
∧ SystemDatenklassifizierung′ = SystemDatenklassifizierung ⊕ {SystemMetadatenEingabe? ↦ (Datenklassifizierung SystemMetadatenEingabe?)})
∨
((Datenklassifizierung SystemMetadatenEingabe?) ∉ CIDDATENKATEGORIEN
∧ CIDSpeichersystemeIds′ = CIDSpeichersystemeIds
∧ SystemDateninhalte′ = SystemDateninhalte ⊕ {SystemMetadatenEingabe? ↦ SystemDateninhaltEingabe?}
∧ SystemDatenklassifizierung′ = SystemDatenklassifizierung ⊕ {SystemMetadatenEingabe? ↦ (Datenklassifizierung SystemMetadatenEingabe?)})
∨
(SystemLandEingabe? ≠ SCHWEIZ ∧ (Datenklassifizierung SystemMetadatenEingabe?) ∈ CIDDATENKATEGORIEN
∧ CIDSpeichersystemeIds′ = CIDSpeichersystemeIds
∧ SystemDateninhalte′ = SystemDateninhalte ⊕ {SystemMetadatenEingabe? ↦ XXXXX}
∧ SystemDatenklassifizierung′ = SystemDatenklassifizierung ⊕ {SystemMetadatenEingabe? ↦ GESCHUETZT})
)
└

┌ RolleHinzufuegen
ΔBANK
RolleEingabe?: ROLLE
MetadatenEingabe?: METADATEN
│
Rollen′ = Rollen ∪ {(RolleEingabe?, MetadatenEingabe?)}
Datenklassifizierung′ = Datenklassifizierung
VerantwortlicheEinheiten′ = VerantwortlicheEinheiten
BenutzerZugriffsrechte′ = BenutzerZugriffsrechte
Teams′ = Teams
InterneBenutzer′ = InterneBenutzer
ExterneBenutzer′ = ExterneBenutzer
└

┌ BenutzerHinzufuegen
ΔBANK
benutzer?: BENUTZER
einheit?: EINHEIT
│
Teams′ = Teams ∪ {(einheit?, benutzer?)}
BenutzerZugriffsrechte′ = BenutzerZugriffsrechte
Rollen′ = Rollen
InterneBenutzer′ = InterneBenutzer
ExterneBenutzer′ = ExterneBenutzer
Datenklassifizierung′ = Datenklassifizierung
VerantwortlicheEinheiten′ = VerantwortlicheEinheiten
└

┌ InternenBenutzerHinzufuegen
ΔBANK
benutzer?: BENUTZER
│
InterneBenutzer′ = InterneBenutzer ∪ {benutzer?}
ExterneBenutzer′ = ExterneBenutzer
Teams′ = Teams
BenutzerZugriffsrechte′ = BenutzerZugriffsrechte
Rollen′ = Rollen
Datenklassifizierung′ = Datenklassifizierung
VerantwortlicheEinheiten′ = VerantwortlicheEinheiten
└

┌ ExternenBenutzerHinzufuegen
ΔBANK
benutzer?: BENUTZER
│
ExterneBenutzer′ = ExterneBenutzer ∪ {benutzer?}
InterneBenutzer′ = InterneBenutzer
Teams′ = Teams
BenutzerZugriffsrechte′ = BenutzerZugriffsrechte
Rollen′ = Rollen
Datenklassifizierung′ = Datenklassifizierung
VerantwortlicheEinheiten′ = VerantwortlicheEinheiten
└

┌ BenutzerZugriffsrechtHinzufuegen
ΔBANK
BenutzerEingabe?: BENUTZER
RolleEingabe?: ROLLE
│
BenutzerZugriffsrechte′ = BenutzerZugriffsrechte ∪ {(BenutzerEingabe?, RolleEingabe?)}
Rollen′ = Rollen
Datenklassifizierung′ = Datenklassifizierung
VerantwortlicheEinheiten′ = VerantwortlicheEinheiten
Teams′ = Teams
InterneBenutzer′ = InterneBenutzer
ExterneBenutzer′ = ExterneBenutzer
└

┌ BenutzerZugriffsrechtEntfernen
ΔBANK
BenutzerEingabe?: BENUTZER
RolleEingabe?: ROLLE
│
BenutzerZugriffsrechte′ = BenutzerZugriffsrechte \ {(BenutzerEingabe?, RolleEingabe?)}
Rollen′ = Rollen
Datenklassifizierung′ = Datenklassifizierung
VerantwortlicheEinheiten′ = VerantwortlicheEinheiten
Teams′ = Teams
InterneBenutzer′ = InterneBenutzer
ExterneBenutzer′ = ExterneBenutzer
└

```
┌ AufSystemdatenZugreifen
  ΞSYSTEM
  ΞBANK
  BenutzerEingabe?: BENUTZER
  BenutzerLandEingabe?: LAND
  SystemIdEingabe?: SYSTEMID
  SystemZugriffMetadatenEingabe?: METADATEN
  InhaltAusgabe!: ℙ INHALT
│
  SystemIdEingabe? = SystemId
  ∧
  SystemZugriffMetadatenEingabe? ∈ Rollen⦇(BenutzerZugriffsrechte⦇{BenutzerEingabe?}⦈)⦈
  ∧
  (
  (SystemDatenklassifizierung⦇{SystemZugriffMetadatenEingabe?}⦈ ⊆ CIDDATENKATEGORIEN ∧
BenutzerLandEingabe? ≠ SCHWEIZ
  ∧ InhaltAusgabe! = {XXXXX})
  ∨
  ((SystemDatenklassifizierung⦇{SystemZugriffMetadatenEingabe?}⦈ ∩ CIDDATENKATEGORIEN
= ∅ ∨ BenutzerLandEingabe? = SCHWEIZ)
  ∧ InhaltAusgabe! = SystemDateninhalte⦇{SystemZugriffMetadatenEingabe?}⦈)
  )
└
```

```
┌ AufMassendatenZugreifen
  ΞBANK
  ΞSYSTEM
  ΔCIDMASSENZUGRIFFSLOG
  BenutzerEingabe?: BENUTZER
  SystemIdEingabe?: SYSTEMID
  BenutzerLandEingabe?: LAND
  MasseninhaltAusgabe!: ℙ INHALT
│
  (
  SystemIdEingabe? = SystemId
  ∧ ROLLEMASSENZUGRIFFCID ∈ BenutzerZugriffsrechte⦇{BenutzerEingabe?}⦈
  ∧ BenutzerLandEingabe? = SCHWEIZ
  ∧ ran SystemDatenklassifizierung ∩ CIDDATENKATEGORIEN ≠ ∅
  ∧ CIDMassenzugriffslog′ = CIDMassenzugriffslog ∪ {(BenutzerEingabe?, SystemIdEingabe?)}
  ∧ MasseninhaltAusgabe! = ran SystemDateninhalte
  )
  ∨
  (
  SystemIdEingabe? = SystemId
  ∧
  (ROLLEMASSENZUGRIFFCID ∈ BenutzerZugriffsrechte⦇{BenutzerEingabe?}⦈ ∨
ROLLEMASSENZUGRIFFNICHTCID ∈ BenutzerZugriffsrechte⦇{BenutzerEingabe?}⦈)
  ∧ ran SystemDatenklassifizierung ∩ CIDDATENKATEGORIEN = ∅
  ∧ CIDMassenzugriffslog′ = CIDMassenzugriffslog
  ∧ MasseninhaltAusgabe! = ran SystemDateninhalte
  )
└
```

┌ MassenCIDZugriffsberechtigungListe
  ΞBANK
  ΞSYSTEM
  MassenCIDBenutzer!: ℙ BENUTZER
│
  MassenCIDBenutzer! = dom (BenutzerZugriffsrechte ▷ {ROLLEMASSENZUGRIFFCID})
└