METADATA-BOUND LIBRARIES ZUGRIFFSSCHUTZ FÜR SAS DATEN

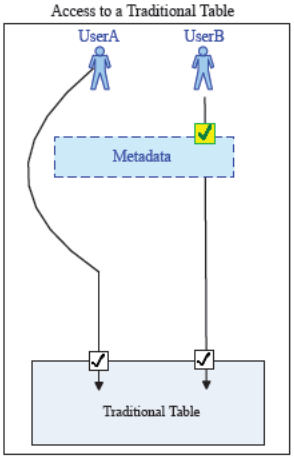
MARKUS TRUNK, SAS SYSTEMARCHITEKT
SAS PLATTFORM NETZWERK, 19 APRIL 2013

AGENDA

- Warum überhaupt Metadata-Bound Libraries ?
- Voraussetzungen
- Funktionsweise, Setup, Autorisierung
- Key-Optionen
- Passwörter
- Best Practice
- Neue Features mit SAS 9.4
- Zusammenfassung

METADATA BOUND LIBRARIES

WARUM ÜBERHAUPT METADATA-BOUND LIBRARIES ?



- **Zugriffslevel auf SAS Dateien erhöhen.**
  Mit SAS Foundation und einem einfachen Libname Statement kann man auf SAS Dateien zugreifen, unabhängig davon welche Berechtigungen für den User, bzw. für die SAS Daten im Metadaten Server gesetzt wurden. Der User kann so die komplette Metadaten-Umgebung umgehen/aushebeln (UserA)
- **Key-Funktion der Metadata-Bound Libraries:**
  Direkten Zugriff auf SAS Data Sets limitieren, bzw. ohne gültige Metadaten Autorisierung verhindern.

METADATA-BOUND LIBRARIES

VORAUSSETZUNGEN

- **Für die Administration:**
  - SAS Version ab 9.3 M2
  - SAS Metadaten Server
  - SAS Management Console
  - Rechte auf File-Ebene sowie für SAS Umgebung

VORAUSSETZUNGEN

- **Für den User-Zugriff auf Metadata-Bound Library:**
  - SAS Version ab 9.3 M2
  - Zugriff auf den Metadaten Server
  - Der Benutzer besitzt alle notwendigen Metadaten Berechtigungen (Authorization Check)
  - Der Benutzer besitzt die notwendigen Rechte auf File-Level-Ebene (Betriebssystem)

METADATA BOUND LIBRARIES — FUNKTIONSWEISE

- Eine Metadata-Bound Library ist ein physikalischer Ordner (Verzeichnis) der fest mit einem Metadaten Objekt (SAS Secured Library) verknüpft wurde.
- Mit “PROC AUTHLIB” und dem CREATE Statement wird ein neues Metadaten Objekt erzeugt (Secured Library) und mit einem Verzeichnis auf Betriebssystemebene verknüpft.
- Jede physikalische Tabelle in einer Metadata-Bound Library enthält Informationen im Header die auf ein dazugehörendes Metadaten Objekt (Secured Table Object) verweisen, d.h. dieser Pointer generiert eine sichere Verbindung zwischen den physikalischen Tabellen auf Betriebssystemebene und den SAS Metadaten.
- Der Zugriff auf Metadata-Bound Tabellen ist somit ohne den dazugehörenden Metadaten-Server nicht möglich, unabhängig davon mit welcher SAS Applikation der User auf die Daten zugreift.

METADATA BOUND LIBRARIES

SETUP

- **Step 1: Secured-Folder anlegen**
  Über die Management Console in den SAS-Folders einen passenden Ordner unter "*/System/Secured Libraries"* erstellen. (Pfad ist fest vorgegeben!)
- **Step 2: Berechtigungen anpassen**
  Berechtigungen für den/die Ordner (Step 1) entsprechend den Anforderungen anpassen, z.B. Abteilung A nur lesen, Abteilung B ändern etc.
- **Step 3: Metadata-Bound Library erzeugen** (SAS Code)

```
Proc authlib;
    create
        library=libtest              → libref der SAS Base Library / Bezug zu den phys. Tabellen
        securedfolder='SecFolder'    → SAS Folder unter /System/Secured (Step 1)
        securedlibrary='SecLib'      → wird automatisch unter /System/Secured/SecFolder angelegt
        pw=secret;                   → Passwort
run;
```


METADATA-BOUND LIBRARIES

SETUP KRITERIEN

- Folgende Kriterien müssen zutreffen damit Proc AUTHLIB ausgeführt werden kann.
  - Die SAS Session läuft unter einem Account der entsprechende Rechte auf die OS-Folder besitzt
    - UNIX: Owner des Verzeichnisses
    - Windows: Vollzugriff auf das Verzeichnis
    - z/OS: Owner des Verzeichnisses
  - *ReadMetadata* und *WriteMetadata* auf die Secured Folders

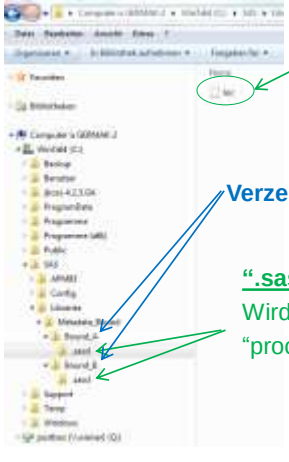
METADATA BOUND LIBRARIES | SETUP

Bild 1 - **vor** PROC AUTHLIB

Bild 2 - **nach** PROC AUTHLIB

- **Nach PROC AUTHLIB**
  - Die generierten Security-Informationen der physikalischen Library (OS Ebene) bestehen aus einem Unterordner (**.sassl**) und einer Datei (**loc**).
    Das dazugehörende Metadaten-Objekt ist das “Secured Library Object”. In Bild 2 ist ***seclib*** das “Secured Library Object” und “***sensitive data***” das Gegenstück auf Betriebssystemebene.
  - Die “Metadata Security-Informationen” für eine physikalische SAS Tabelle werden im Datei-Header gespeichert.
    Das korrespondierende Metadaten-Objekt ist das “Secured Table Object”. In Bild 2 sind ***tableA*** und ***tableB*** die Secured Table Objects und ***tableA.sas7bdat*** und ***tableB.sas7bdat*** die verknüpften physikalische SAS-Tabellen.

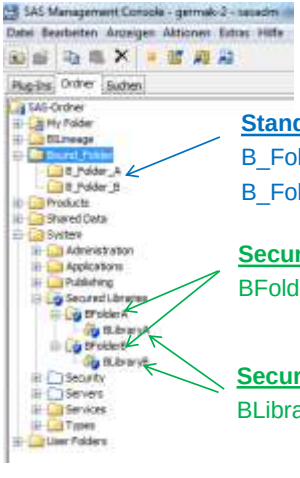
METADATA-BOUND LIBRARIES | SETUP



Inhalt der Datei: “loc”
480224C1-F455-4E07-9BBA-48489B6F09D1/System/SecuredLibraries/BFolderA/BLibraryA

Verzeichnis auf OS-Ebene

“.sassl” Ordner u. “loc” Datei
Wird mit dem “create” Statement von “proc authlib” erzeugt



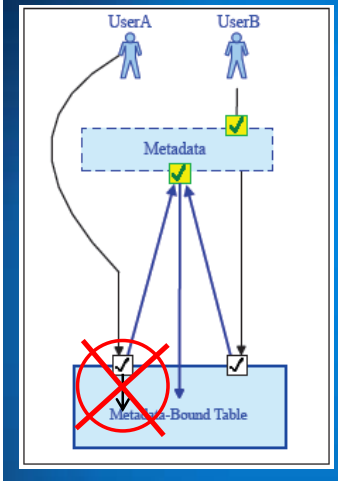
Standard SAS Folders
B_Folder_A u. B_Folder_B

Secured Folders
BFolderA u. BFolderB

Secured Libraries
BLibraryA u. BLibraryB

METADATA-BOUND LIBRARIES

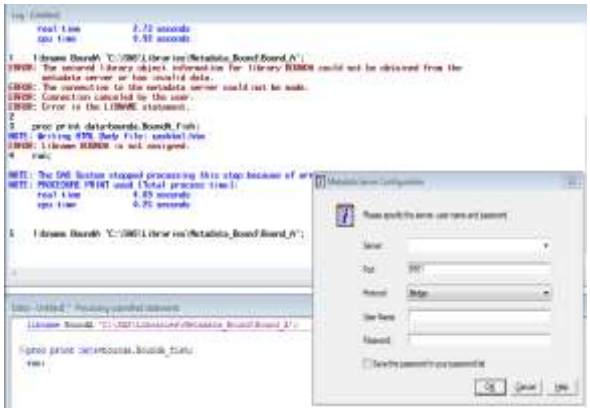
AUTORISIERUNG



- Nachdem die Metadata-Bound Library erfolgreich erstellt wurde, ist ein direkter Zugriff auf die Daten nicht mehr möglich.
- Durch die Security-Informationen im File-Header und der dazugehörende Secured Library (Security Binding) wird der Access-Request zwingend an den Metadaten-Server zur Autorisierung weitergeleitet

METADATA-BOUND LIBRARIES

AUTHORIZATION



- Ohne gültige Anmeldung am Metadata-Server erscheint beim Daten-Zugriff eine entsprechende Anmeldemaske.
- Mit gültiger Anmeldung am Metadata-Server erfolgt der Zugriff auf die Daten wie gehabt (seamless).

PROC AUTHLIB - KEY OPTIONEN

- Proc AUTHLIB – Create
- Proc AUTHLIB – Report
- Proc AUTHLIB – Modify
- Proc AUTHLIB – Remove
- Proc AUTHLIB – Tables
- Proc AUTHLIB – Repair (Preproduction)

KEY OPTIONEN - PROZEDUREN

- Proc AUTHLIB – Create
  - Erstellt das “Secured Library Object” in den SAS Metadaten und erzeugt die notwendigen Security-Informationen und Verknüpfungen auf File-Level Ebene.
- Proc AUTHLIB – Report
  - Erstellt eine Liste mit dem Inhalt der “Secured Library” (Dateinamen, Secured Table Name, SecuredTableID sowie mögliche inkonsistente oder korrupte Meta-Bound Verbindungen
- Proc AUTHLIB – Modify
  - Setzt das Library Passwort (oder Passwörter) für alle ungesicherten (unbounded) Tabellen.
  - Erneuert das Passwort (oder Passwörter), so dass es mit der Metadata-Bound Library übereinstimmt

KEY OPTIONEN - PROZEDUREN

- Proc AUTHLIB – Remove
  - Das Remove Statement entfernt alle physikalischen Security Informationen von der Library sowie aus den SAS Tabellen (Table Header)
  - Das Remove Statement löscht die zusammengehörenden Secured Libraries und Secured Table Objects
- Proc AUTHLIB – Tables
  - Gibt die Tabelle innerhalb einer Metadata-Bound Library an die aktualisiert oder entfernt werden soll
- Proc AUTHLIB – Repair (Preproduction)
  - Wiederherstellen (Recovery) von Security Informationen einer physikalischen Tabelle, einer Secured Library oder Secured Table Objects

PASSWÖRTER

- Metadata-Bound Libraries benötigten ein Passwort oder ein Satz von Passwörtern
  - Passwörter werden in den physikalischen Daten und in den Metadaten gespeichert
  - Passwörter werden nur verschlüsselt gespeichert oder übermittelt.
  - Passwörter können nicht für die Zugriffssteuerung verwendet werden (Authentifizierung)
  - Mit Proc PWENCODE können Passwörter in der AUTHLIB Prozedur verschlüsselt werden.
  - Benutzer müssen das Passwort an keiner Stelle eingeben, bzw. kennen.

METADATA BOUND LIBRARIES — PASSWORT DETAILS

- Alle Tabellen in einer Metadata-Bound Library besitzen das gleiche Passwort, bzw. Passwort-Set
  - Wenn das Ziel der neuen Tabelle eine Metadata-Bound Library ist, wird dieses (Ziel)Library-Passwort auf die kopierte Tabelle automatisch übernommen.
  - Beim Kopieren in eine traditionelle SAS Library wird das Passwort nicht übertragen und die Tabelle ist nicht mehr durch Metadata-Bound Security geschützt.
- Es gibt drei Passwörter für Metadata-Bound Libraries, angelehnt an das READ-, WRITE- und ALTER Passwort für SAS Data Sets
  - Zur Vereinfachung wird empfohlen nur ein einzelnes (single) Passwort mit "PW=[*all-passwords]*" zu setzen und nicht unterschiedliche Passwörter für Lesen, Schreiben oder Ändern zu verwenden.
  - Das Passwort für die "PW=" kann aus max. 8 Zeichen bestehen
  - Werden alle drei Passwörter gesetzt (read, write, alter) können bis zu 24 Zeichen verwendet werden

METADATA BOUND LIBRARIES — PASSWÖRTER AUF SAS DATA SETS

Syntax Beispiel:

- Metadata-Bound Libraries erstellen - SAS Data Sets sind durch ein Passwort geschützt

```
Proc authlib lib=libtest;
      create securedfolder='SecFolder'
      securedlibrary='SecLib'
      pw=[bestehendes data set PW] / [Metadata-Bound PW];
run;
```

- Metadata-Bound Library erstellen - SAS Data Sets sind mit verschiedene Passwörtern für read, write, alter geschützt.

```
Proc authlib lib=libtest;
      create securedfolder='SecFolder'
      securedlibrary='SecLib'
      pw=[Metadata-Bound PW] oder [read= write= alter=];
table test1 / pw=abc;                    → für data set test1 wurde ein single PW=abc gesetzt
table test2 / read=abcd write=efgh alter=ijkl;   → für data set test2 wurde ein PW für read, write und alter gesetzt
table test3;                             → für data set test3 wurde kein PW gesetzt
run;
```

METADATA BOUND LIBRARIES

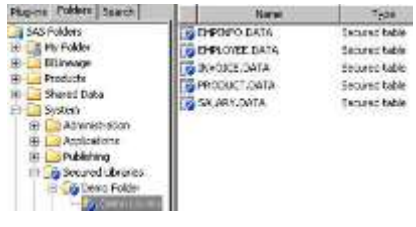
BEST PRACTICE

- SAS Tabellen zwingend mit SAS Tools verwalten (erstellen, löschen, kopieren etc.) - nicht auf OS-Ebene. Ausnahme für File-Recovery.
- Rechte auf den */System/Secured Libraries Folders* einschränken
- Bei dem Einsatz von Metadaten Promotion z.B. für Dev, Test und Prod sollte für jede Umgebung eine eigene Kopie der physikalischen Daten vorgesehen werden.
- Bei dem Erstellen oder Anpassen von Metadata-Bound Libraries sollten die physikalischen Daten nicht im Zugriff sein
- “Secured Data Folders”, “Secured Library Objects” und “Secured Tables objects” in das Backupkonzept mit aufnehmen
- SAS 9.3 Guide to Metadata-Bound Libraries

METADATA-BOUND LIBRARIES

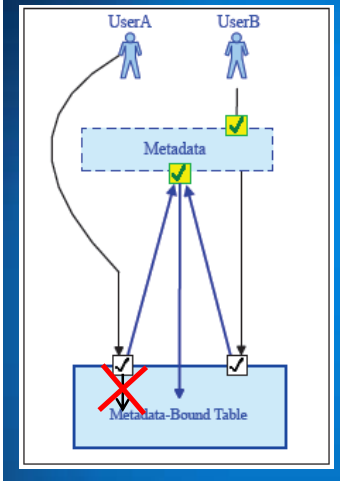
NEUE FEATURES MIT SAS 9.4

- **Verwalten der Metadata-Bound Libraries über die SAS Management Console**
  - Metadata-Bound Libraries erzeugen, verwalten, löschen, überprüfen



- **Erweiterte Encryption Optionen für PROC Authlib (mit SAS 9.4 M1)**

METADATA-BOUND LIBRARIES



ZUSAMMENFASSUNG

- Kein Zugriff auf SAS Dateien ohne gültige Metadaten Autorisierung
- Der Zugriffsschutz ist persistent, d.h. die Security-Einstellungen werden immer wieder an die Tabelle mit dem selben Namen innerhalb der Library weitergegeben, auch wenn die Datei z.B. auf Betriebssystemebene gelöscht und neu erstellt wurde.
- Das Passwort ist nur für die Erstellung und Verwaltung der Metadata-Bound Libraries notwendig, nicht für den User-Zugriff
- Support für Windows, Unix und z/OS
- Voraussetzung SAS Version ab 9.3 M2