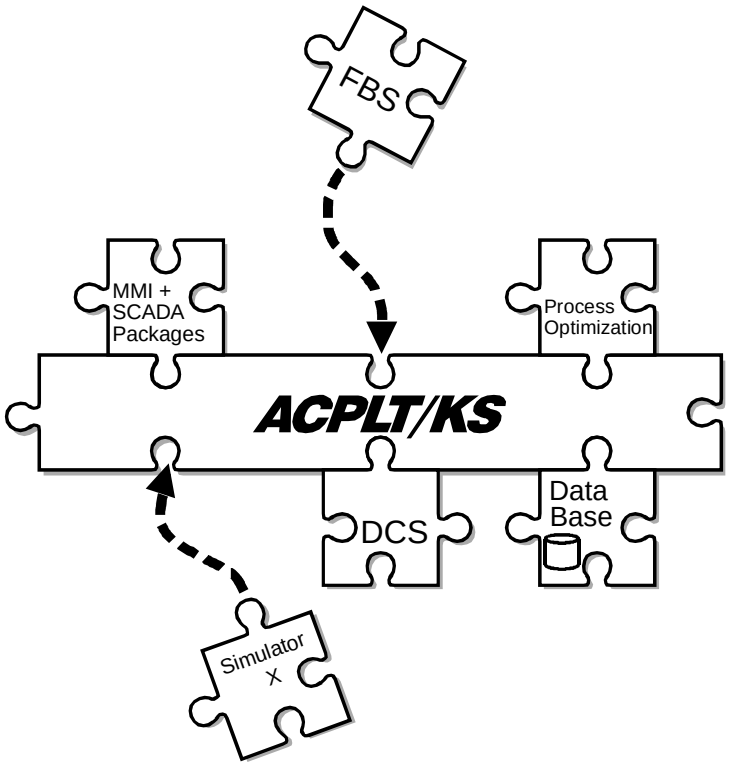
ACPLT/KS

Technologiepapier Nr. 7:
A/V-Module



Inhalt

Technologiepapier Nr. 7 – Ausgabe 01.97.1
ersetzt: Ausgabe 12.96.1

Ansprechpartner: H. Albrecht
Lehrstuhl für Prozeßleittechnik der RWTH Aachen
D-52056 Aachen
Tel.: +49 241 80-7703
Fax.: +49 241 8888-238
eMail: ks@plt.rwth-aachen.de
WWW: http://www.plt.rwth-aachen.de/ks

1 Einleitung

Das Kommunikationssystem ACPLT/KS (im folgenden „KS“ genannt) verbindet im Bereich von Anwendungen der Prozeß- und Betriebsführung rechnergestützte Werkzeuge untereinander und mit Prozeßleitsystemen. Dieses Technologiepapier beschreibt den Einsatz von zusätzlichen Modulen zur Authentifikation/Verifikation bei Diensteanforderungen.

2 A/V-Module

Beim Kommunikationssystem ACPLT/KS erfolgt ein Zugriffsschutz auf Basis von sogenannten „Authentifizierungs-/Verifikations-Modulen“ (A/V-Module). Damit können beispielsweise unberechtigte Zugriffe auf Parametersätze von Reglern verhindert werden. Die Authentifikation/Verifikation erfolgt bei ACPLT/KS bei jedem übertragenen Datenblock (Diensteanfrage beziehungsweise -antwort).

Dazu definiert das KS-Kernprotokoll, an welcher Position innerhalb einer Diensteanfrage oder -antwort die A/V-Informationen übertragen werden. Dieses Technologiepapier spezifiziert für das Kernprotokoll nur zwei einfache A/V-Mechanismen, die jeder KS-Server implementieren muß:

- Beim NULL-A/V-Modul findet weder eine Authentifikation noch eine Verifikation statt.
- Beim SIMPLE-A/V-Modul erfolgt die Authentifizierung über eine einfache Zeichenkette (Passwort/Kennung). Eine Verifikation der Echtheit findet jedoch auch hier nicht statt. Außerdem wird die Zeichenkette unverschlüsselt übertragen.

```
enum KS_AUTH_TYPE {
    KS_AUTH_NONE   = 0, /* NONE-A/V-Modul   */
    KS_AUTH_SIMPLE = 1  /* SIMPLE-A/V-Modul */
};
```

Das KS-Kernprotokoll ist um zusätzliche A/V-Module erweiterbar, die aber nicht verpflichtend in jedem Server oder Klienten implementiert sein müssen. Die Vergabe der Ident-Nummern zur Kennzeichnung des zu verwendenden A/V-Moduls erfolgt zentral über den Lehrstuhl für Prozeßleittechnik.

3 Versand von A/V-Daten innerhalb des Kernprotokolls

Zu Beginn jeder Serviceanforderung schickt der Klient A/V-Informationen in der nachfolgend aufgeführten Datenstruktur mit. Erst darauf folgen die dienstespezifischen Parameter.

```
union KS_AUTH_REQ switch (KS_AUTH_TYPE type) {
    case KS_AUTH_NONE:
        void;
    case KS_AUTH_SIMPLE:
        KS_AUTH_SIMPLE_REQ simple;
};
```

Die Diensteantworten eines KS-Servers beginnen standardisiert ebenfalls immer mit Authentifizierungsinformationen in Form der Datenstruktur `KS_AUTHRES` (siehe auch Abbildung 3.1). Darauf folgt der Fehlercode und gegebenenfalls ein weiterer – dienstespezifischer – Datenblock.

```
union KS_AUTH_REPLY switch (KS_AUTH_TYPE type) {
    case KS_AUTH_NONE:
        void;
    case KS_AUTH_SIMPLE:
        void;
};
```

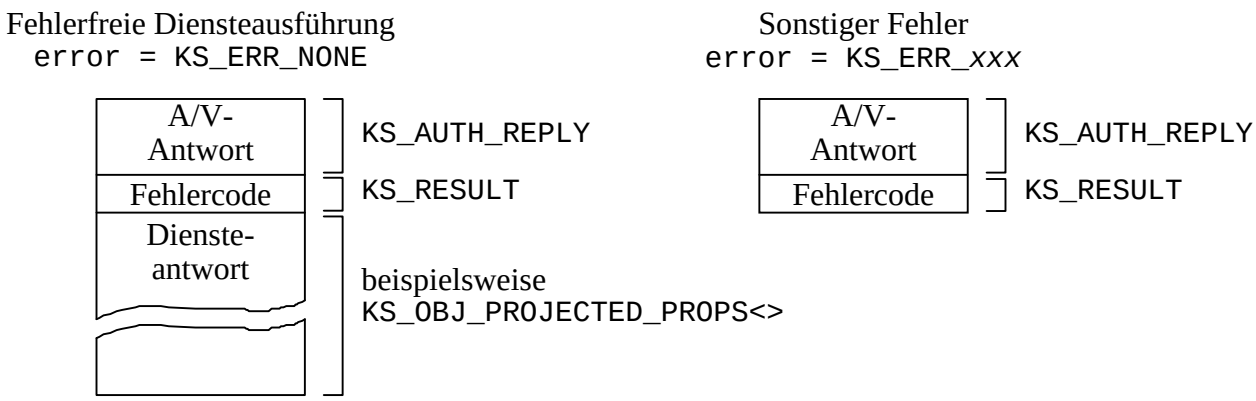


Abbildung 3.1: *Typischer Aufbau einer Diensteantwort am Beispiel des* KS_GETPP-*Dienstes.*

Mit Hilfe der Datenstruktur KS_AUTH_REPLY ist es möglich, daß besondere A/V-Module im Klienten sowie im Server jederzeit sogenannte „Credentials“ auffrischen oder andere Abgleichvorgänge vornehmen können. Außerdem ist auf diese Weise auch eine Authentifizierung/Verifikation des Servers gegenüber dem Klienten denkbar.

3.1 NULL-A/V-Modul

Beim NULL-A/V-Modul werden keinerlei A/V-Informationen zwischen dem Klienten und dem Server ausgetauscht. Jeder Klient kann ohne weitere Kontrolle jeden Dienst auf einem Server ausführen.

3.2 SIMPLE-A/V-Modul

Das SIMPLE-A/V-Modul ermöglicht eine einfache Zugangskontrolle zu den Server-Diensten auf Basis eines Kennwortes (beziehungsweise Benutzerkennung). Das SIMPLE-A/V-Modul sieht keine Maßnahmen zur Verifikation der Echtheit der Benutzerkennung vor.

Die Benutzerkennung besteht aus einer beliebigen Zeichenkette von bis zu maximal 255 Zeichen Länge. Die Zeichenkette darf nur aus „druckbaren“ ASCII-Zeichen mit Zeichencodes zwischen 32 (Leerfeld) und 126 (Tilde) bestehen. Dieses Technologiepapier trifft jedoch keine Annahmen über die Interpretation dieser Zeichenkette, die beispielsweise als eine einfache Benutzerkennung oder auch als eine durch ein besonderes Zeichen getrennte Liste von Kennungen interpretiert werden kann.

```
const KS_SIMPLEID_MAXLEN = 255;

struct KS_AUTH_SIMPLE_REQ {
    string id<KS_SIMPLEID_MAXLEN>;
};
```

4 Implementierungshinweise

Die Namen (Kennungen) der in einem KS-Server verfügbaren A/V-Module kann ein KS-Klient über die Variable "av_modules" innerhalb des "vendor"-Zweiges des Kommunikationsobjektbaumes erfragen. Existiert diese Variable nicht, so sind im betreffenden Server nur die

A/V-Module "none" und "simple" vorhanden. Eine Erläuterung der hinter dem Variablennamen in eckigen Klammern angegebenen Eigenschaften ist in [1] nachzulesen.

Variable "/vendor/av_modules" [OPT, PA, RO]

Diese Variable vom Typ KS_VT_STRING_VEC enthält eine Liste der Kennungen von A/V-Modulen, die der Server unterstützt. Vom Kernprotokoll werden nur die Kennungen "none" sowie "simple" definiert.

Bei der Verwendung von A/V-Modulen kann die folgende Fehlermeldung auftreten:

KS_ERR_UNKNOWNAUTH = 0x0005

Der Klient benutzt in seiner Serviceanforderung ein A/V-Schema, das dem Server unbekannt ist oder von diesem nicht unterstützt wird.

Die Diensteantwort eines KS-Servers muß immer das gleiche A/V-Modul benutzen, das der Klient bei der Diensteanfrage verwendete. Tritt jedoch der Fehler KS_ERR_UNKNOWNAUTH auf, so muß die Diensteanwort das NULL-A/V-Modul benutzen.

5 AuA – Abkürzungen und Akronyme

ACPLT/KS	Kommunikationssystem des Lehrstuhls für Prozeßleittechnik der RWTH Aachen
IP	Internet Protocol
ISO	International Standards Organization
ONC	Open Network Computing
OSI	Open Systems Interconnect
RPC	Remote Procedure Call/Calling
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
XDR	External Data Representation

6 Literaturverzeichnis

[1] ACPLT/KS Group:
Technologiepapier #6: Implementierungshinweise
Lehrstuhl für Prozeßleittechnik, RWTH Aachen, 1996