4.1.1 Verbindungsaufbau zwischen Primärsystem und Konnektor

Die Kommunikation zwischen Primärsystem und Konnektor basiert auf den Protokollen

- HTTP (verpflichtend),
- CETP (optional) und
- LDAP (verpflichtend)

Am Konnektor kann die Absicherung der Verbindung in 4 Stufen konfiguriert werden [gemSpec_Kon#3.4] – von keiner Absicherung in Stufe 1 bis zur vollständigen Absicherung in Stufe 4. Nur bei Stufe 4 können alle Funktionen der TI genutzt werden. Stufen 1 bis 3 sind mit funktionalen Einschränkungen verbunden.

Die vier Konfigurationen wirken auf HTTP folgendermaßen (mit Konnektor als TLS-Server und Primärsystem als TLS-Client):

Tabelle 2: Tab_ILF_PS_Konfigurationsvarianten_HTTP

Stufe 1	TLS deaktiviert. Verwendung von HTTP ohne Absicherung auf Transportebene
Stufe 2	TLS mit Server-Authentisierung ohne Client-Authentisierung.
Stufe 3	TLS mit Server-Authentisierung ohne Client-Authentisierung. HTTP mit Basic Authentication, d. h. Client-Authentisierung auf Ebene von http mit Username und Passwort. Das Primärsystem muss Username und Passwort für die Basic Authentication statisch konfigurieren, so dass eine Übereinstimmung mit der Konfiguration am Konnektor besteht.
Stufe 4	TLS mit Server-Authentisierung und Client Authentication. Die Client-Authentisierung muss mit den Zertifikaten erfolgen, die am Konnektor erzeugt wurden und vom Administrator in das Primärsystem importiert wurden oder mit konnektorfremden X.509-Zertifikaten der Primärsysteme, die über das Managementinterface in den Konnektor eingespielt wurden.

Für die CETP-Verbindung (mit Primärsystem als TLS-Server und Konnektor als TLS-Client) gibt es zwei Konfigurationsvarianten: