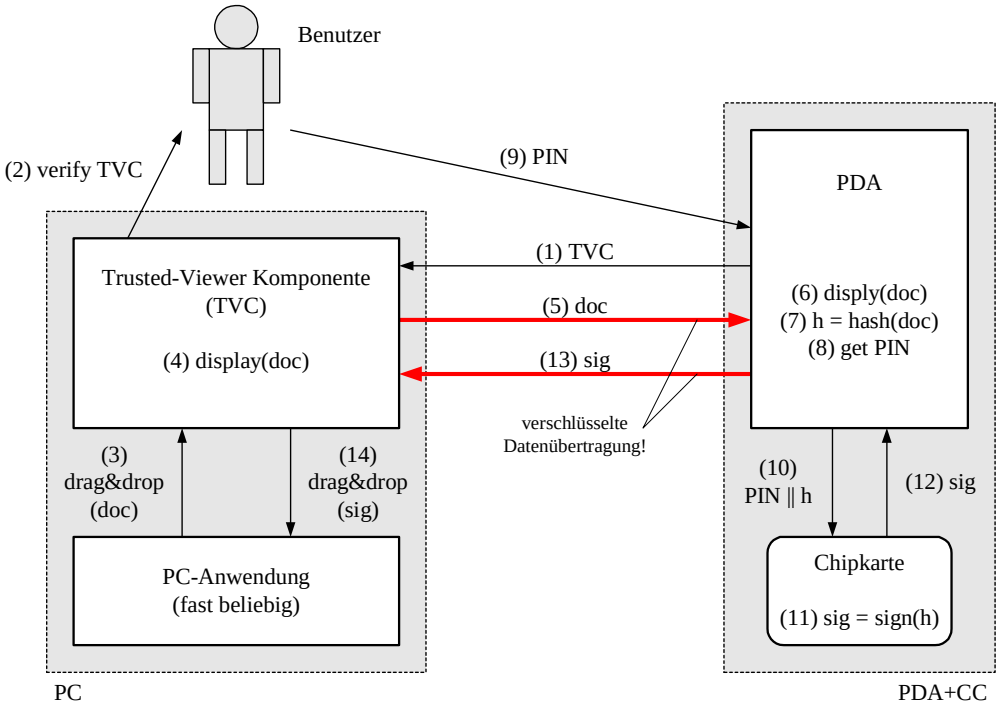
Trusted Viewer

Im Rahmen der Erstellung von digitalen Signaturen (nicht nur nach SigG bzw. SigV) ist es erforderlich, dem Benutzer das entsprechende Dokument vor der „Unterzeichnung“ vertrauenswürdig anzuzeigen; gewünscht ist: „What you see is what you sign“. Es gilt Angriffe zu verhindern, bei denen dem Benutzer zunächst ein harmloses Dokument angezeigt wird, er aber letztendlich ein völlig anderes Dokument digital signiert.

In diesem 4h-Praktikum soll der PDA das Dokument mit Hilfe einer Chipkarte signieren (diese Komponente ist bereits vorhanden). Die Anzeige des Dokuments soll auf einem PC (der potentiell unsicher ist) erfolgen. Hierzu wird der so genannte Trusted Viewer zunächst vom PDA auf den PC geladen und dort gestartet. Der Viewer authentifiziert sich nun gegenüber dem Benutzer und empfängt das zu signierende Dokument. Nachdem das Dokument verschlüsselt vom PC zum PDA übertragen wurde, wird es am PDA signiert. Die resultierende Signatur wird anschließend wieder zum PC übertragen.



Voraussetzungen:

- Fundierte Kenntnisse der Programmiersprache Java
- Grundkenntnisse der Systemsicherheit (z.B. VO Systemsicherheit)
- Grundkenntnisse der PDA-Programmierung
- Grundkenntnisse der Chipkarten-Programmierung (z.B. PDA- & CC-Labor) sind von Vorteil.

Teilnehmer:
2 Studierende Informatik

Ansprechpartner:
Dr. Peter Schartner (E.1.51, DW 3718, e-Mail: peter.schartner@uni-klu.ac.at)