Im RC2 der AusweisApp 1.9.5 Testversion durchgeführte Anpassungen und Ergänzungen:

1. Im (unwahrscheinlichen dennoch möglichen) Falle, dass der Benutzer die Online-Authentisierung abbricht, bevor das CV-Zertifikat da ist (bevor die erste DIDAuthenticate ankommt) und aber der TCToken abgeholt wurde, wird die Ermittlung der RefreshURL nicht im Bezug auf SubjectURL aus der CertificateDescription, sondern auf TCTokenURL laufen. Die Hashwerte der ermittelten SSL-Zertifikate werden in diesem Falle nicht geprüft, da die Referenz-Werte fehlen.

2. Während der Überprüfung der RefreshURL wird die letzte URL (nach Algorithmus der Wert der Variable "Location" im letzten "Redirect"-Response) nicht auf Konformität zu der Same-Origin-Policy geprüft.

=> Diskussion und Klärung dieses Punktes im DIF eCard-API.

3. Die Grenze für den TCToken ist auf 20 KB gesetzt.

(Kein Spezifikations-relevanter Punkt, ist aber als Verhalten der AA so mit BSI abgestimmt)

4. Die AA ist im Falle des SAML-Szenarios in Bezug auf SAML vollkommen "ahnungslos" - das Protokoll läuft völlig transparent durch.

5. Bei SOAP wird davon ausgegangen, dass die refreshAddress aus dem TCToken URL direkt zu der RefreshURL wird -> Same-Origin-Policy ist damit erfüllt.

6. Das Zertifikat der RefreshURL wird nicht mehr mit Hilfe von HTTP-Get abgegriffen, sondern es wird nur ein TLS-Handshake mit dem Server realisiert.

7. Im Kapitel 3.4.2 sind nur HTTP-Response-Codes 302, 303 und 307 zugelassen, 301 - Moved permanently nicht. Wir hatten schon einen Support-Fall, in dem die AA 301 vom Server erhalten hat. In diesem Fall wird die AusweisApp einen Fehler auswerfen.

=> Diskussion und Klärung dieses Punktes im DIF eCard-API.

8. Der RC2 wird die Java Version 1.7.0 u9 unterstützen.