kantara INITIATIVE

Ruth Puente <ruth@kantarainitiative.org>

[WG-IDAssurance] Service availability criterion applicability flaw

Richard G. WILSHER (@Zygma) <RGW@zygma.biz> Thu, Sep 6, 2018 at 5:08 PM
To: IA WG <wg-idassurance@kantarainitiative.org>

I realized only yesterday that there is a long-standing structural flaw in the Classic SAC (IAF-1400) which has some new consequences.

Observation: the existing criterion ALn_CM_CSM#040 Status Information Availability states that [An enterprise and its specified service must:]

Provide, with [95|99]% availability, a secure automated mechanism to allow relying parties to determine credential status and authenticate the Claimant's identity.

The problem I initially realized is that, since this criterion lies within the IAF-1400 OP_SAC Part E (Credential Status Management), any Component Service which does not provide credential status management functionality avoids having to meet any availability criterion. I believe that any service should be subject to this availability requirement, and that therefore this criterion should be placed where it is unambiguously applicable to all CSPs, irrespective of their type of the extent of its functionality.

The situation was carried forward when we split IAF-1400 into IAF-1410 (CO_SAC) and IAF-1420 (OP_SAC – in which 'CSM#040 now resides). The problem therefore remains for 'Classical' assessments. However, the problem was further compounded when we created the 'NIST 800-63 rev.3' Class of Approval, in which, since IAF-1420 does not apply, there is no longer ANY requirement for service availability (there being none in either IAF-1430 or 1440).

I suggest that the solution is twofold:
1) introduce into IAF-1410 (which is intended to apply to all Classes of Approval) a new criterion, utilizing the tag of one long-since withdrawn:
AL[2|3|4]_CO_ISM#110 [CO#235 @AL3] Service Availability

Be provided with at least [95|99]% availability.

Note that I am deliberately NOT proposing any such criteria at AL1 (there is no 'ISM' set of criteria); and
2) withdraw ALn_CM_CSM#040 in IAF-1420.

I'm quite surprised that this has never been previously raised, even though it must have been there forever (probably since tScheme days? – hence I'm specifically included you, RJT, fyi).

I don't expect this to be addressed during today's meeting, but wanted to put it on the record while it was on my mind. I suggest that we address it such that it can be resolved by amendment to criteria at the time that any other SAC tweaks are released.
I will join today if able – likely on the road.

Best,

Richard G. WILSHER
Founder & CEO

Operating independently since 1993

M: +1 714 797 99 42
E: RGW@Zygma.biz
W: www.Zygma.biz
