Porter, Rachel

From: Barra, Lynn
Sent: Wednesday, February 22, 2017 9:52 AM
To: Porter, Rachel
Cc: Barra, Lynn
Subject: FW: [comments] Public Review Comments - INCITS 499-201x - additional comments from James Sellwood

Importance: High

From: James Sellwood [mailto:james.sellwood.2010@live.rhul.ac.uk]
Sent: Sunday, February 19, 2017 10:06 AM
To: Barra, Lynn
Cc: drbenigni47@gmail.com; Francomacaro, Salvatore (salvatore.francomacaro@nist.gov)
Subject: Re: [comments] Public Review Comments - INCITS 499-201x

Hello Lynn,

Thank you for letting me know. I have two further comments which I'd be grateful if you'd pass on:

The XACML standard and the 2014 NIST Guide to Attribute Based Access Control (ABAC) Definition and Considerations both include support for environmental input into the authorization evaluation. In fact the NIST guide includes such support as part of its definition of ABAC. In contrast, the draft NGAC functional architecture specification makes no mention of such input to the decision. I wondered what was the reasoning behind this exclusion. It seems highly plausible that context associated with the system and the environment may be desired input to the evaluation process. Time of day (compared to working hours or specific user/object constraints) is already available within some systems, and other examples seem equally viable.

In Section 6.2.4 (Relations) a process is explicitly identified in respect of negative relations (i.e. prohibitions and restrictions) as well as obligations, but it never mentioned in respect of positive relations (i.e. assignments, associations, privileges, capabilities, and ACEs). It is unclear whether the omission of processes from positive relations is intentional. However, it is noticeable given their mention throughout the other relations.

Many Thanks

James

James Sellwood