GLOBALPLATFORM
THE STANDARD FOR SMART CARD INFRASTRUCTURE
GlobalPlatform, Inc.
544 Hillside Road
Redwood City, CA 94062 USA

LS to OMA

Title:	Response to Liaison Statement from OMA OMA-LS_942-OMA_ARC_Reply_to_GlobalPlatform_on_Secure_Element_access_control-20120223-A.doc
Source:	GlobalPlatform
To:	OMA-ARC-SCT, Mr Patrice Beaudou
Cc:	OMA-LIAISON@mail.openmobilealliance.org OMA-CD-CMAPI – Mr Thierry Berisot
Contact person:	Gil BERNABEU (GlobalPlatform Technical Director)
Document Number:	GPD_LS_019
Date:	05 April 2012

OMA problem statement

OMA has advised GlobalPlatform of their interest in using access control to protect access to NAAs in the secure elements used for network access. In this model several SEs could be used, including legacy SIMs and RUIMs. In this latter case, OMA is concerned that Access Control mechanism defined by GlobalPlatform might not be possible because of the lack of an application identifier (AID).

Response from GlobalPlatform

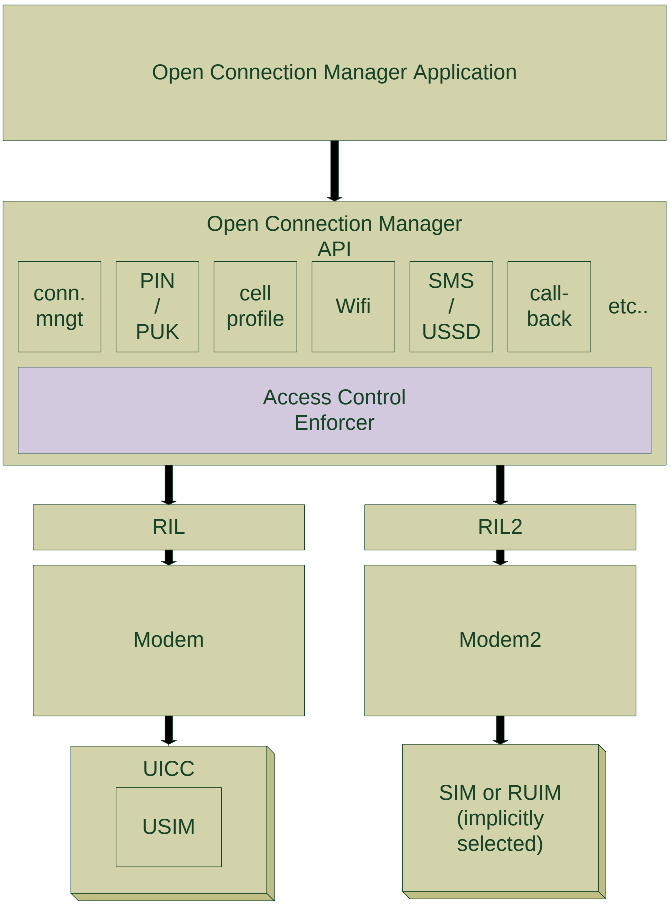
GlobalPlatform SE Access Control working group thinks that secure element access control might be used in the context of OMA's Open Connection Manager enabler, with certain limitations however.

First GlobalPlatform wishes to remind OMA that the GlobalPlatform SE access control specification makes certain assumptions on the device OS, mostly that :
- applications are signed
- device OS can be trusted to
    - enforce signature check and provide accurate information
    - bypassing access control is not possible by directly accessing lower layers

Some of the above might not be applicable in some of the OSs that OMA is targeting, in particular personal computers.

Proposed implementation

Access control enforcer must be implemented in the device OS, sitting between access to the secure element and the third party applications requesting access. Hence we foresee the following architecture for use of the access control with the Open Connection Manager API and applications:



Following this implementation, both DF/EF type NAAs (SIM, RUIM) and application-style NAAs (e.g. USIM) can be protected by access control:

- For the SIM or RUIM: by using the “default selected application” semantics.
- For the other NAAs: by specifying their AID in the access control rules.

Please note that the public review version of the SEAC specification uses the term "default selected", which is inconsistent with the term used in GlobalPlatform Card Specification v2.2.1, where the mechanism is named "implicit selection". Alignment of the wording in the SEAC specification will be considered after the public review.

The current public review ends April 15 and GlobalPlatform welcomes comments from OMA members.

GlobalPlatform looks forward to a fruitful cooperation with OMA.