AUTOMOTIVE IDENTITY

HIGH LEVEL DESCRIPTION

Automotive Identity High Level Description

Version 1.0

03 June 2021

This is a White Paper of the GSMA

Security Classification: Non-confidential

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those permitted under the security classification without the prior written approval of the Association.

Copyright Notice

Disclaimer

The GSM Association ("Association") makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Compliance Notice

The information contain herein is in full compliance with the GSM Association's antitrust compliance policy.

Table of Contents

1 Introduction

The Automotive Identity (AiD) project is focused on exploring the possibilities of enabling mobile, content and automotive services to be easily federated and provisioned into cars and accessed via authentication[1].

In particular, one of the key aims is to enable individuals to seamlessly use their mobile subscription[2] and mobile services via an in-car system and consumer eSIM, thereby mitigating some of the challenges of using smartphones reliably in cars for telephony and connectivity services (discussed further in Annex A.2).

Not only does this provide an elegant solution for in-car connectivity[3], but also opens up innovative business models around car sharing in which the personalized settings and services of a user can easily be transferred between different cars of a car sharing fleet on user entry.

Whilst the AiD framework will be explored using automotive as a leading use case to guide the user stories and functional requirements, the aim is that the framework should be extensible to other industry sectors and use cases.

This document represents the first phase of the project in which a feasibility study has been conducted on the Automotive Identity concept to identify the actors, user stories, core processes and potential deployment topologies based on the consumer eSIM specification[4]. Later phases may go on to deliver technical specifications for the AiD framework and proposals for enhancements to particular standards used within the AiD framework (such as SGP.21/22).

It should be noted that this document identifies and discusses a number of different topologies and implementation options for the AiD framework divided into two separate categories (see section 4) – the intention is not that an implementation of the AiD framework support all the topologies and options but rather to highlight different approaches that might form a basis for specification of the AiD framework at a later stage.

[1] Single factor, 2-factor or multi-factor as required

[2] Either an existing mobile subscription or one specifically for use within the AiD service

[3] Note that this is separate from the M2M connectivity that may be provided to a vehicle for telematics and emergency calling services

[4] The AiD framework is rooted in the consumer eSIM specification in contrast to using SIMs or the M2M eSIM specification

1.1 Document scope

In Scope	Out of Scope
• Automotive identity (AiD) service definition & proposition • Definition of roles/actors & user stories • Core processes • AiD framework categories & associated topology options • Additional considerations (security; privacy etc.) • Potential enhancement areas applicable to the specifications	▪ Implementation guidelines ▪ Detailed technical specifications ▪ Go-To-Market business models and considerations ▪ Methods of authentication (implementation-specific) ▪ Proposal for enhancements of specifications[5]

Table 1: Document scope

1.2 Abbreviations

Term	Description
AiD	Automotive Identity
App	Appplication
AUP	AiD User Profile
BT	Bluetooth
CLI	Calling Line Identity
CMP	Car Mobility Provider (such as fleet management, automotive manufacturer or car sharing provider)
CPM	Converged IP Messaging
CRM	Customer Relationship Management
CTAP	Client to Authenticator Protocol
DI	DownloadInfo
EID	eUICC ID
eUICC	Embedded Universal Integrated Circuit Card
FIDO	Fast IDentity Online
HMI	Human Machine Interface
M2M	Machine to Machine
MEP	Multiple Enabled Profiles
MSP	Mobile Service Provider

[5] The AiD framework focuses on delivering new user journeys, some of which might require enhancements to existing standards.

Term	Description
OEM	Original Equipment Manufacturer
OMA	Open Mobile Alliance
OP	(RSP) Operational Profile
OS	Operating System
OTA	Over The Air
QoS	Quality of Service
RSP	Remote SIM Provisioning
RPM	Remote Profile Management
UE	User Equipment (i.e., handset, mobile phone)
UX	User experience
VASP	Value Added Service Provider

Table 2: Abbreviations

1.3 Definitions

Term	Description
AiD service	Service provided to a user that enables them to provision a car with usage of a mobile subscription and a collection of services from the MSP, CMP and other VASPs and access these capabilities and services within different cars
AiD 3rd party service	MSP, CMP, VASP services provided within the AiD service
AiD framework	Framework used for delivering the AiD service
AiD User Profile	Single profile encompassing the user's services & preferences and MSP metadata[6] that is downloaded into a car to enable that car to be personalised to that user
Car details	Information about the car making it distinguishable from other cars in the context the car details are evaluated. E.g. car make & model in a list of privately owned cars or EID provided to the MSP for preparation of an RSP Operational Profile (OP)
CMP	Car Mobility Provider: entity that administers usage of the AiD service within designated cars (e.g., auto OEM/car dealership, fleet management, car rental service etc.)
CMP user account	Account that a user has with their CMP for managing their AiD User Profile (and associated RSP Operational Profiles) and the vehicles in which they have been provisioned
DownloadInfo	The information needed by the Car to initiate download and installation of an RSP Operational Profile in order to access the related mobile subscription within the Car

[6] E.g., MSP name, icon etc. for display via the Car HMI

Term	Description
Mobile subscription	Commercial relationship between the Subscriber and the Operator/Service Provider
Mobile info	Information and metadata encompassing the user's info, value-added service entitlements and user preferences (AiD 3rd party services) that are shared by the MSP with the CMP during onboarding for incorporation & use within the AiD User Profile that is downloaded to the car to personalise it to the user
MSP	Mobile Service Provider: entity supporting the AiD service and providing a user's existing mobile subscription and services
MSP user account	Account that a user has with their MSP for managing their mobile subscription(s) and value-added services (e.g., via an app or self-care portal)
MSP_token	A time-limited token (unique per mobile subscription) that may be provided by an MSP to a CMP during user onboarding to the AiD service that enables the CMP to make API requests to the MSP to perform actions on behalf of the user
Multi-device service	An end-user service provided by the MSP that involves the Car and other user devices, such as a smartphone (e.g., Active Call Handover)
RSP Operational Profile	A combination of Operator data and applications to be provisioned to the Car eUICC for the purpose of providing mobile services by the Operator [SGP.21/22]
User	An entity, not part of the AiD system, which uses AiD system services

Table 3: Definitions

1.4 References

Ref	Doc Number	Title
[1]	N/A	In-car Mobile Signal Attenuation Measurements, Ofcom UK, https://www.ofcom.org.uk/__data/assets/pdf_file/0019/108127/in-car-mobile-signal-attenuation-report.pdf
[2]	TR 38.901	Study on channel model for frequencies from 0.5 to 100 GHz
[3]	TS.43 v6	Service Entitlement Configuration
[4]	SGP.21 v2.2	RSP Architecture
[5]	SGP.22 v2.2.2	RSP Technical Specification

Table 4 : References

1.5 Actors

The following actors are defined within the AiD framework:

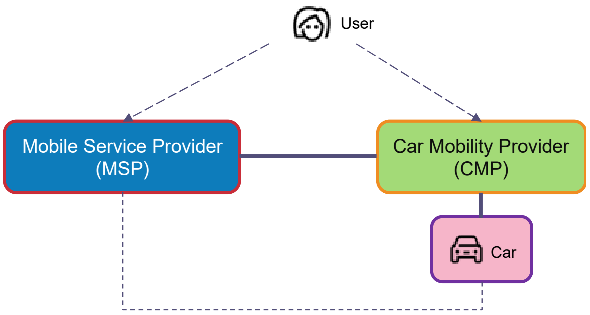


Figure 1 AiD actors

User:

- An individual using the AiD service within one or more Cars
- Establishes or uses an existing mobile subscription with a Mobile Service Provider (MSP) for use with the AiD service
- Registers with a Car Mobility Provider (CMP) able to support the Car(s) in which the user wishes to use the AiD service
- Generates an AiD User Profile with the CMP for personalising the Car(s) to the user
- Links their mobile subscription to the AiD User Profile for use in the Car(s)
- Manages the AiD service via the MSP and CMP as appropriate

MSP (Mobile Service Provider):

- Provides the user with a mobile subscription associated with the AiD service
- Onboards the user to the AiD service in conjunction with the CMP
- Provides information as needed to the CMP for generating the AiD User Profile with the user and setting up the AiD service
- Provisions the Car eUICC with an RSP Operational Profile (OP) for the mobile subscription on user request
- Supports lifecycle management of the AiD service

CMP (Car Mobility Provider):

- Onboards the user in conjunction with the MSP to the AiD service
- Enables the user to set up their AiD User Profile for use within the Car(s) linked to the CMP
- Provisions the AiD User Profile to the target vehicle
- Supports lifecycle management of the AiD service

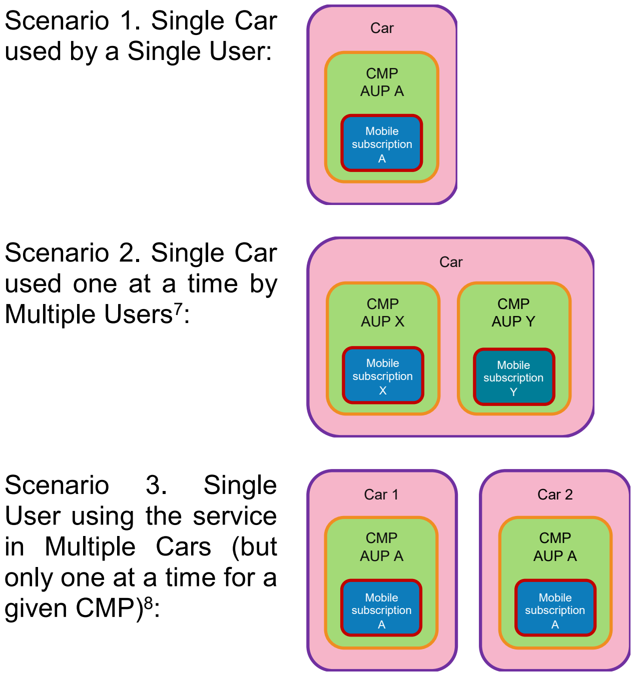
Car:

- Interfaces with a CMP and MSP to support:
  - Personalisation of the Car to the user based on the AiD User Profile downloaded to the Car

  - Provisioning of an RSP Operational Profile into the Car eUICC to enable the user to access their mobile subscription via the Car
- Provides an authentication mechanism through which the user can access their AiD User Profile and associated OP in the Car
- Supports an AiD User Profile (and OP) per individual hence enabling multiple people to have personalised use of the Car

1.6 Overview of scenarios

The AiD framework is intended to support a number of implementation scenarios based on the Actors identified in the previous section.



Scenario 1. Single Car used by a Single User:

Scenario 2. Single Car used one at a time by Multiple Users[7]:

Scenario 3. Single User using the service in Multiple Cars (but only one at a time for a given CMP)[8]:

Figure 2 AiD Service scenarios

These scenarios are discussed in more detail in section 2 – User Stories.

1.7 Key goals

- Enable federation of a user's mobile subscription, services and preferences via a single AiD User Profile (AUP) – referred to as the AiD service
- Enable provisioning of this AUP into a new Car upon user request, including provisioning of an eUICC within the Car with the user's OP
- Enable the user to access their AiD service (i.e., the AUP and OP) in the Car via authentication[9]

[7] Same or different MSPs (user choice)

[8] Same or different CMPs depending on ability of a given CMP to support the target Car

[9] Single-factor, two-factor or multi-factor as required

- Allow for both the new Car (when enabled with the user's OP) and the user's smartphone to be simultaneously active and enabled on the mobile network to support multi-device services[10]
- Enable the user to bring their AiD service with them as they move between different cars managed by the CMP
- Enable the user to link their mobile subscription with multiple AiD User Profiles so that they can use it with different cars and different CMPs
- Enable multiple users to have individual use of the Car via their respective AiD User Profiles (and associated OPs); only one user can access their AiD service within the Car at a time
- Define an AiD framework and candidate topologies that can deliver on these functional requirements
- Ensure that the framework minimises friction in the user journey wherever possible (i.e., reducing the number of user interactions needed to perform a particular function)
- Ensure that the AiD framework builds on top of already deployed solutions where applicable
- Leverage existing standards (e.g., OpenID Connect; eSIM standards; OMA CPM[11]; TS.43 ODSA etc.) and design patterns where applicable
- Ensure that the AiD framework is easy to integrate with and scalable

2 User stories

2.1 Prerequisites

- The user has a mobile subscription with an MSP that they are able to use with the AiD service
- The Car in which the user wants to use the AiD service has the necessary capabilities for supporting the AiD service:
  - CMP app preloaded
  - Existing connectivity e.g., via a Provisioning profile on the Car (consumer) eUICC, or via the M2M eUICC in order to be able to facilitate provisioning of the user's AiD User Profile and OP into the Car
  - Is able to provide a secure mechanism for authenticating the user
- If the subscriber's offer includes multi-device services (Car+smartphone), both the user‘s car and the user's smartphone must be technically capable to support the services

[10] Where supported by the user's MSP, smartphone and target device

[11] Open Mobile Alliance Converged IP Messaging

2.2 AiD service onboarding

Ref	User Story	Actor	Comments
1.1	User can discover the AiD service via a range of different channels (MSP app/portal; CMP app/portal)	MSP; CMP	MSP and CMP determine the channels and touchpoints made available to users.
1.2	User registers with a CMP	MSP; CMP	Users registers with a CMP appropriate to their needs and the cars they would like to use the AiD service with (e.g., an Auto OEM, Car Rental company etc.). User generates an AiD User Profile (AUP) that will be used to encompass the services and preferences they would like to use within a Car.
1.3	User onboards to the AiD service	MSP; CMP	The onboarding process links a user's specific mobile subscription at an MSP to their AiD User Profile with a CMP. Onboarding can be instigated either starting at the MSP or CMP touchpoint (e.g., smartphone, tablet/desktop) with redirects as necessary to the other entity to ensure a single user journey[12]. Mechanisms must be in place to authenticate the user to the MSP, verify that the user has authority to request the AiD service for the designated mobile subscription and that the mobile subscription is eligible for the AiD service. As part of the onboarding process, information and metadata pertaining to the user, their services and their service preferences may be shared with the CMP to aid the user in generating their AiD User Profile and setting up the AiD service. Users can onboard without needing to have a target Car at the point of onboarding - for instance, in the case of car rental. If the user is able to stipulate a target Car during onboarding, the eligibility of this Car can be checked (e.g., AiD functionality, multi-device support etc.). In the case where the AiD service offering incorporates multi-device services that have a dependency on a user's other devices (such as the user's smartphone), the eligibility of such devices may be checked during the onboarding process.

2.3 Car provisioning

Ref	User Story	Actor	Comments
2.1	User requests a new Car to be added to their AiD service	MSP; CMP; Car	Car eligibility checked to ensure compliance with the AiD service. User must have first onboarded and registered for an account with a CMP able to support the target Car.

[12] The flow will require selection/discovery of the MSP (for flows starting at CMP) and vice versa

Ref	User Story	Actor	Comments
2.2	AiD User Profile and associated information related to the mobile subscription is provisioned and enabled within a new Car after the user authenticates to their AiD service and requests use of the AiD service within that Car	CMP; MSP, Car	User authenticates to the CMP and easily gains access to their AiD service within the Car. Car eligibility checked to ensure compliance with the AiD service. User must have first onboarded and registered for an account with a CMP able to support the target Car. If the AiD service offering includes multi-device services (involving the Car and other user devices), the eligibility of such devices can also be checked.
2.3	Authentication mechanism established within the Car for the user to access their AiD service	Car; CMP	Establishes an authentication mechanism within the Car through which the user can authenticate to access their AiD service (i.e., enable their AiD User Profile and associated OP for use within the Car).
2.4	User wishes to add a new Car but has exhausted the number of cars permissible within their AiD service	MSP; CMP; Car	User wishes to activate a new Car but has exhausted the number of cars permissible in their AiD service: • AiD framework includes a mechanism for removing an existing Car from the user’s AiD service (e.g., least-used or user-stipulated) and/or • User is able to stipulate which Car to remove from their AiD service portfolio
2.5	User wishes to add their AiD service to a new Car but the Car eUICC does not have a free slot to add the user’s OP	CMP; Car, MSP	A mechanism is required for removing one or more OPs from the Car eUICC.

2.4 AiD service enablement/disablement (daily car usage)

Ref	User Story	Actor	Comments
3.1	User activates their AiD service on Car-entry by authenticating	CMP; Car	User authenticates in the Car to access their AiD service in that Car.
3.2	Multiple users are able to use their AiD service within a Car	Car	The Car supports multiple users, and only makes a particular AiD User Profile (and associated OP) available when a user successfully authenticates to that AiD User Profile. Only one user at a time is able to use their AiD service in a particular Car.
3.3	AiD service is disabled when the user exits the Car	Car	For instance: • User manually logs out before exiting the Car • AiD service is disabled when the Car is locked by the user (physical key, digital key)

2.5 AiD service removal from a Car

Ref	User Story	Actor	Comments

4.1	User requests the removal of their AiD service from a specific Car	MSP;
		CMP;
		Car
			Results in the deactivation/removal of the AiD User Profile and OP. Can be explicit or implicit depending on scenario.
			Example scenarios:
			• End of car rental period
			• User is selling the car
			• User has exhausted the number of cars they can provision with their AiD service hence needs to remove one of them from their AiD service portfolio

4.2	CMP instigates a request to remove a particular AiD User Profile (and associated OP) from a specific Car	CMP; MSP, Car	CMP instigates request to remove the AiD User Profile (and associated OP) of a particular user from a specific Car; removal actioned once consent from the affected user has been obtained. Example scenarios: • User has exhausted the number of cars permissible within their AiD service but wishes to use their AiD service in a new Car hence the MSP/CMP needs to remove one of the user's existing cars from their AiD service portfolio • Car eUICC does not have a free slot for adding the mobile subscription of a new user wanting to use their AiD service in the Car • Car rental company needs to remove all profiles and return the Car to the 'factory reset' state ready for the next customer • AiD User Profile and/or OP in the Car is faulty and needs to be replaced
4.3	MSP instigates a request to replace an OP within a specific Car	MSP; Car	MSP may need to instigate removal of an OP if for example the OP is faulty and needs replacing

2.6 AiD service lifecycle

Ref	User Stories	Actor	Comments

5.1	Mobile subscription becomes unavailable	MSP;
		CMP;
		Car
			User attempting to use their AiD service in a Car is notified by the Car of a lack of connectivity.
			User may still be able to administer their AiD service via the MSP and CMP touchpoints.

5.2	User requests their AiD service to be cancelled	MSP;
		CMP;
		Car
			AiD service account (and associated AiD User Profile) temporarily disconnected or deleted for that user.

Ref	User Stories	Actor	Comments
5.3	User re-joins the AiD service	MSP; CMP	AiD service account for that user re-activated if available (i.e., if the account was suspended rather than deleted when the user previously left the AiD service); otherwise, user onboards as per 1.3.
5.4	User administration of the AiD service	MSP; CMP	User able to review which Cars are active within their AiD service (MSP; CMP).
5.5	User wishes to migrate their AiD service (i.e., AUP & mobile subscription) to a new Car	MSP; CMP; previous Car, new Car	User requests removal of the AiD service from the existing Car (as per 4.1). User requests the AiD service to be added to the new Car (as per 2.1 or 2.2) The user may also need to register with and onboard to the AiD service with a new CMP if their existing CMP is unable to support the new Car (as per 1.2).
5.6	User churns from one MSP to another	Previous MSP; new MSP CMP	User requests their AiD service to be cancelled with their current MSP. User onboards to the new MSP, activates the AiD service and links it to their CMP account as per 1.3.
5.7	Device eligibility change	MSP	User notified if a new device (such as a new smartphone) that they are using is unable to support one ore more of the multi-device services supported within the AiD service.
5.8	Changes to a user's AiD User Profile are propagated to all cars where the AiD User Profile has been installed	MSP; CMP; Car	For instance, changes to the AiD 3rd party services encompassed within the AiD service for that user. Note: this story may be limited by some 3rd party services which may not be supported by some cars (eligibility check may be required).
5.9	AiD service supports telephony services within the Car	MSP; CMP; Car	AiD service may be capable of supporting the following services subject to sufficient eligibility[13]: • Data connectivity • Outgoing voice calls originated from the Car (with CLI reflecting user's mobile subscription) • Incoming voice calls received in the Car • Active voice call handover from other user device to the Car system (when entering the Car) • Active voice call handover from the Car system to other user device • Send & receive messages (SMS, MMS, RCS) • Access to a contacts list for use with the telephony services

[13] Subject to MSP capabilities, mobile subscription type & restrictions and the individual capabilities of the car and smartphone for multi-device services.

3 Core AiD processes

This section discusses the processes that the AiD framework will need to provide in order to deliver the AiD service and provides some example flows. Section 4 then identifies two different categories and associated topologies that might be used to deliver on these processes and flows. The following colour-coding is used within the diagrams to differentiate the functions of each actor:

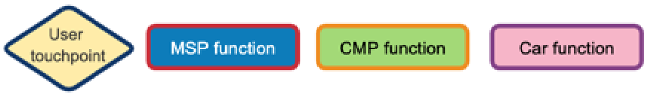


Figure 3 Colour-coding used in AiD diagrams

3.1 User onboarding to the AiD service

User onboarding can be instigated either via the MSP or the CMP.

Example CMP-orientated onboarding flow:

- User registers to the CMP and subscribes to the AiD service
- User stipulates their MSP, or MSP is determined by other means
- CMP redirects user to their MSP
    - MSP authenticates user and obtains their authorisation to use their mobile subscription with the AiD service
- MSP redirects user back to CMP
- MSP may provide the user's 'mobile info'[14] to the CMP to support the onboarding process and AiD service setup
- CMP finalises onboarding process with the user (e.g., AiD User Profile setup) and notifies the user accordingly
- The user may also receive a confirmation notification from their MSP

[14] Information and metadata encompassing the user's info, value-added service entitlements (AiD 3rd party services) and user preferences that are shared by the MSP with the CMP for incorporation & use within the AiD User Profile that is downloaded to the Car to personalise it to the user

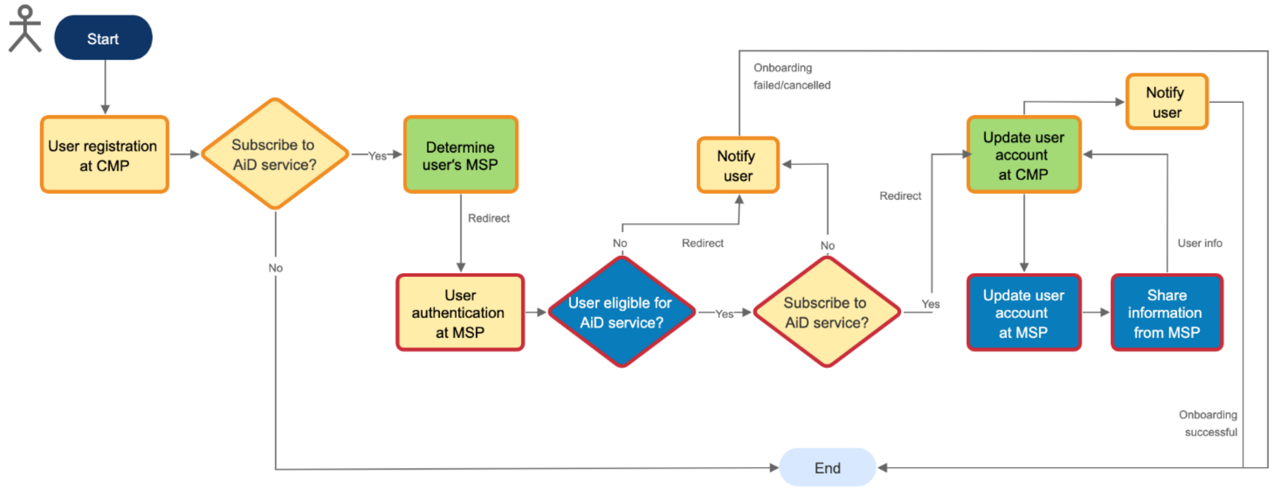

Start
User registration at CMP
Subscribe to AiD service?
Yes
Determine user's MSP
Redirect
User authentication at MSP
User eligible for AiD service?
No
Redirect
Notify user
Onboarding failed/cancelled
Yes
Subscribe to AiD service?
No
Yes
Redirect
Update user account at CMP
Notify user
Update user account at MSP
Share information from MSP
User info
Onboarding successful
No
End

Figure 4 Example Onboarding flow starting at CMP touchpoint

Onboarding starting at an MSP touchpoint could be accommodated via a redirect to the CMP flow outlined above:

- User elects to subscribe to the AiD service via their MSP
- User selects CMP (from those supported by the MSP) and is redirected to the CMP WebPortal and follows the CMP onboarding flow

3.2 Car provisioning with the AiD service

User enters a new Car and wishes to personalise it with their AiD service. An example flow is shown below; note that the flow is indicative and may vary based on the topology used in the deployment of the AiD framework or due to different use cases and/or to meet local regulatory requirements. User confirmation for the provisioning of an OP to the Car eUICC will be obtained within the end-end flow but how this is achieved is topology and implementation dependent.

Example flow:

- User authenticates to the AiD service (via the CMP) in the new Car
- CMP obtains Car details (e.g., EID, Car identifier, Car make & model) either directly from the Car or via a separate database and checks eligibility for the AiD service
- Request issued to the MSP to use the user's mobile subscription in the new car
  - Car details might be passed to the MSP to enable binding of the OP to that particular Car
- MSP determines whether there are any restrictions on provisioning the user's mobile subscription to that particular Car (e.g. eligibility check)
- MSP returns information for initiating the OP provisioning to the CMP/Car, as applicable
- CMP passes the AiD User Profile (and the DownloadInfo where applicable) to the Car
- Car installs the AiD User Profile

- Car uses the received information to instigate the process of downloading and installing an OP in the Car eUICC so that the user can access their mobile subscription within the Car as part of the AiD service
- Car notifies the user that their AiD service has been successfully installed and also notifies the CMP
- CMP sends a status update to the MSP
- CMP and/or MSP may also provide an acknowledgement to the user
- Car must set up a local authentication method with the user for enabling them to securely access their AiD service on Car-entry going forward and to safeguard their privacy in the scenario where the Car is being shared by multiple users.

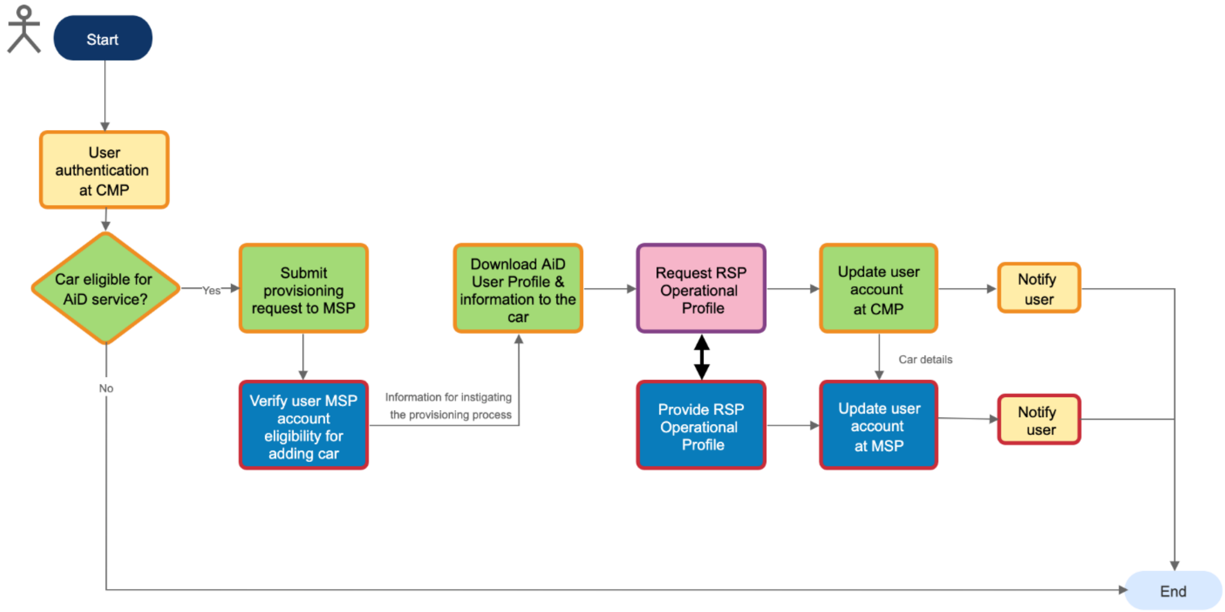

Start
User authentication at CMP
Car eligible for AiD service?
Yes
No
Submit provisioning request to MSP
Verify user MSP account eligibility for adding car
Information for instigating the provisioning process
Download AiD User Profile & information to the car
Request RSP Operational Profile
Provide RSP Operational Profile
Update user account at CMP
Car details
Update user account at MSP
Notify user
Notify user
End

Figure 5 Example flow for Car provisioning

3.3 Enabling AiD service on Car-entry

The user enables their AiD service within a Car as follows (assumes that the Car has already been provisioned with the AiD service and OP):

1. User unlocks the Car
2. User authenticates to their AiD service in-car
3. User confirms enablement of their mobile subscription for use within the AiD service in the Car

Depending on how these steps are implemented, it may be possible to combine them to provide a more streamlined flow for the user. For instance, if the method of unlocking the Car allows for user differentiation (e.g., each car key maps to a unique user), then step 2 could be encompassed within step 1[15]. Separately, the act of authenticating to the AiD service in step 2 could also be used to enable use of the mobile subscription as per step 3.

[15] An initial onboarding step would be needed to link a specific CMP user account (AUP/OP) with a particular 'driver' as recognised by the Car. This process would be implementation specific.

SGP.22 [5] provides more guidance on what level of user confirmation is required for implementation of step 3.

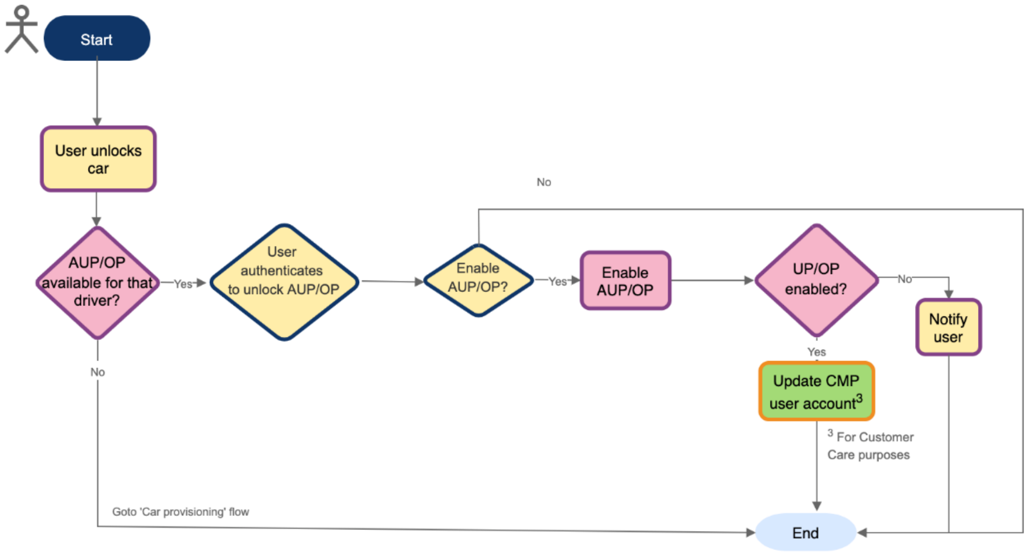

Start
User unlocks car
AUP/OP available for that driver?
Yes
No
User authenticates to unlock AUP/OP
Enable AUP/OP?
Yes
No
Enable AUP/OP
UP/OP enabled?
No
Yes
Notify user
Update CMP user account³
³ For Customer Care purposes
Goto 'Car provisioning' flow
End

Figure 6 Enabling AUP/OP on Car-entry

3.4 Disabling AiD service on Car-exit

The AiD service may be disabled within a Car either by explicit user action (e.g., user disables or 'logs out' via the Car HMI) or implicitly by the user locking the Car (in the scenario where the AUP/OP are linked to a driver profile administered by the Car). CMP may inform the MSP of the change in AUP/OP status.

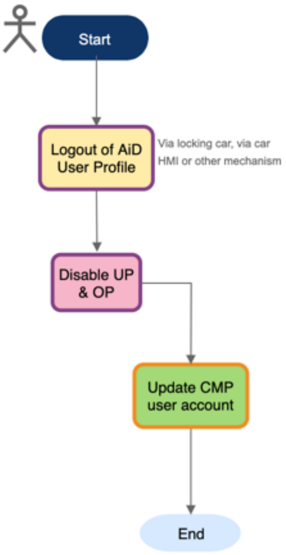

Start
Logout of AiD User Profile
Via locking car, via car HMI or other mechanism
Disable UP & OP
Update CMP user account
End

Figure 7 Disabling AiD User Profile on exiting the Car

3.5 Removing AiD service from a Car

There are a number of situations where the AiD service (i.e., the user's AUP and/or OP) may need to be removed from a Car, as discussed previously in section 0, or in the case where a user wishes to withdraw from the AiD service (see section 3.7):

An example flow is as follows:

1. User authenticates to their MSP and requests removal of their mobile subscription from a specific Car or all Cars
2. MSP deactivates OP for the specified Car
3. OP remains in the Car until a user in the Car (any user) chooses to delete it (e.g., when prompted by the Car to delete other OPs to make space for that user's own OP in the eUICC)
4. Separately, the user authenticates to and instructs the CMP to remove their AUP from the specified Car
5. CMP marks the user's AUP for deletion and this is actioned by the Car (implementation dependent)

[Optionally] the MSP following step 2, may notify the CMP directly that the user has requested removal of their AiD service from the specified Car hence avoiding the user needing to request removal of their AUP directly with the CMP (implementation dependent).

Note: in the above flow, a new OP is generated against the user's mobile subscription for each new Car. A more efficient approach would be to port the user's OP from one Car to another – this may be facilitated in a future iteration of the standards.

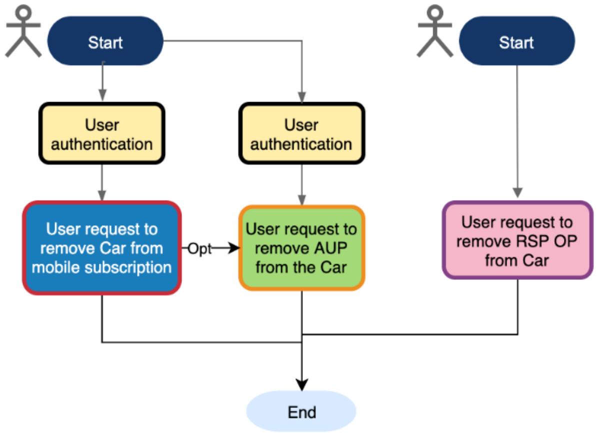

Start
Start
User authentication
User authentication
User request to remove Car from mobile subscription
Opt
User request to remove AUP from the Car
User request to remove RSP OP from Car
End

Figure 8 AiD service removal (example flow)

An OP may need to be removed for other, logistical reasons; for example:

<u>Mobile subscription limit</u>

- The user's mobile subscription may be limited by their MSP in terms of the number of devices/profiles that can be activated against the subscription. The user authenticates to a new Car, but the user has run out of spare slots in their mobile subscription hence before an OP can be downloaded to a new Car, one of the user's existing OPs used in the AiD service must first be deactivated at the MSP. Whether the RSP OP is also removed from the Car eUICC is a matter of implementation.

Car eUICC limit

- User authenticates in a new Car but their OP cannot be downloaded because the Car eUICC has run out of space and is not able to accommodate any additional OPs; in this scenario, the Car will need to remove an OP and may prompt the new user to authorise deletion of an OP to free up space – determination of which OP to delete in such a scenario is left down to implementation.

3.6 Suspend/resume mobile subscription within the AiD service

The MSP may need to suspend/resume or invalidate a mobile subscription for operational purposes. Doing so may impact on the AiD service; an example flow:

- MSP suspends the ability for the user to use their mobile subscription with the AiD service temporarily and notifies them accordingly
- MSP may notify CMP of the AiD service (user) that has been suspended
- Upon Car-entry and after user authentication, the Car may notify the user via the Car HMI that their AiD service is currently available but unconnected

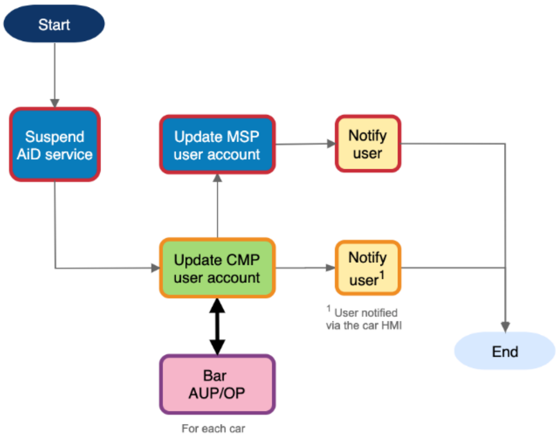


Figure 9 Account status change at MSP

- Once the MSP resumes the AiD service for a given user, it may notify the CMP
- CMP notifies the affected Car(s)
- MSP/CMP notifies the user that their AiD service is now connected again

3.7 User withdrawal from AiD service

- User requests withdrawal from the AiD service (via MSP or CMP)
- AiD service deactivated/removed from each Car in which it was previously provisioned (as per process outlined in section 3.5)

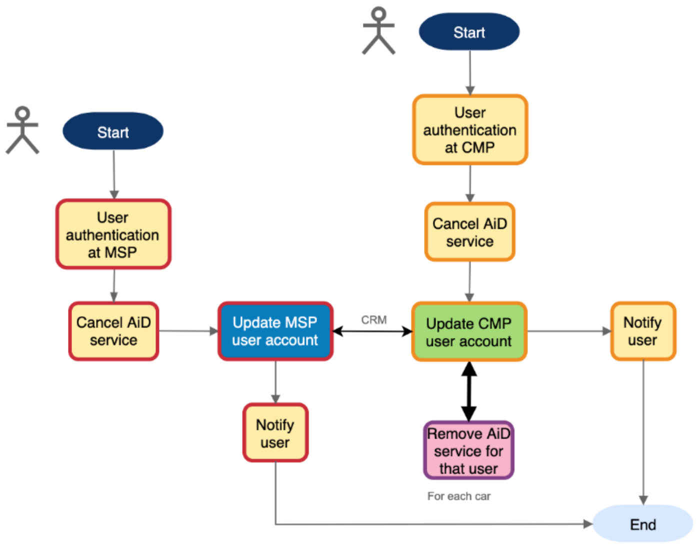


Figure 10 User withdrawal from AiD service

4 AiD framework Categories & Topologies

The AiD service and associated framework will need to be flexible and extensible to encompass a range of different use cases and propositions and allow for different implementations based on individual market requirements, existing infrastructure, business objectives and local regulation.

This section outlines two candidate Categories and associated Topologies that could be considered in the design and deployment of the AiD framework and assesses their applicability based on the proposition outlined in sections 1 and 2. The categories are:

Category A: CMP/MSP account federation

Category B: Smartphone centric

Category A is based on a federation of the users' accounts with the MSP and the CMP and relies on an integration between the MSP backend and the CMP backend for onboarding and provisioning the service. In contrast, Category B uses a CMP app within the smartphone as a central entity for onboarding and provisioning the service for the user.

Both categories rely on the cars providing, to a differing extent, a proprietary or standardised interface within the Car utilised by the CMP application for delivering the AiD service – a common / standardized car interface across the different automotive vendors will be important for the AiD service to scale. Example implementation options illustrating some of these different approaches are included for each of the Categories.

Whilst Category B takes a smartphone-centric approach for provisioning the AiD service into a Car, both categories may use a smartphone as an integral part of the operation of the AiD service; e.g., to provide preferences, playlists, contacts etc. for use within the AiD service in-Car. This aspect is deemed implementation specific and hence out of scope for this document. Account federation between CMP and MSP may be applicable in either Category.

4.1 AiD framework interfaces

This section provides a high level over of the AiD framework and interfaces between the various actors. Note that some of the interfaces described in this section would be defined and used differently depending on the topologies of both Categories.

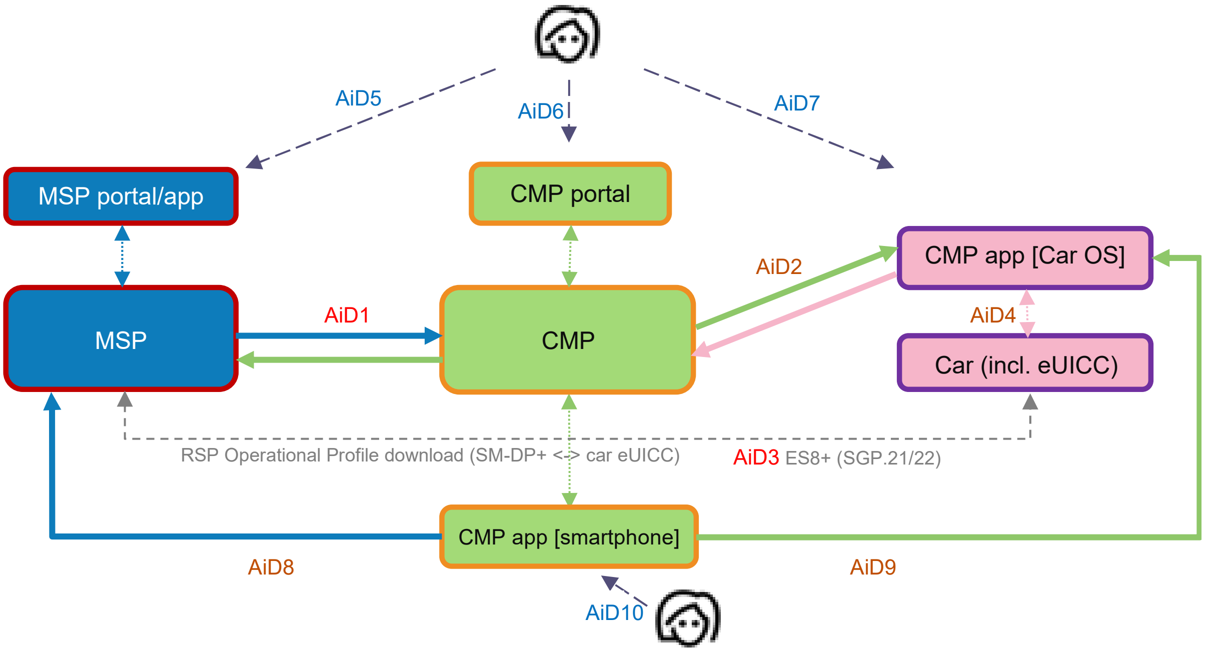


Figure 11 AiD framework interfaces

AiD1 (MSP <-> CMP)

- Managing user onboarding, Car provisioning (depending on Category)
- AiD service lifecycle management

AiD2 (CMP <-> CMP app [Car OS])

- Downloading the AiD User Profile to the Car
- Providing information to enable the CMP app to instigate provisioning of the user's mobile subscription to the Car (where applicable)
- Profile lifecycle management

AiD3 (MSP <-> Car eUICC)

- Secure transport for the delivery of an RSP Operational Profile between the SM-DP+ and the Car eUICC [ES8+ SGP.21/22]

AiD4 (Car <-> CMP application [Car OS])

- Exposure of APIs to a CMP application that runs in the Car OS for AiD service lifecycle management

AiD5 (User <-> MSP)

- Onboarding the user to the AiD service and in-life service management (implementation specific user interface)

AiD6 (User <-> CMP portal)

- Onboarding the user to the AiD service and in-life service management (implementation specific user interface)

AiD7 (User <-> CMP app [Car OS])

- User authentication to the AiD service (Car entry), logout (Car exit) and management of the AiD service within the Car (proprietary user interface administered by the CMP towards the user)

AiD8 (CMP app [smartphone] <-> MSP)

- Managing user onboarding, Car provisioning (depending on Category)

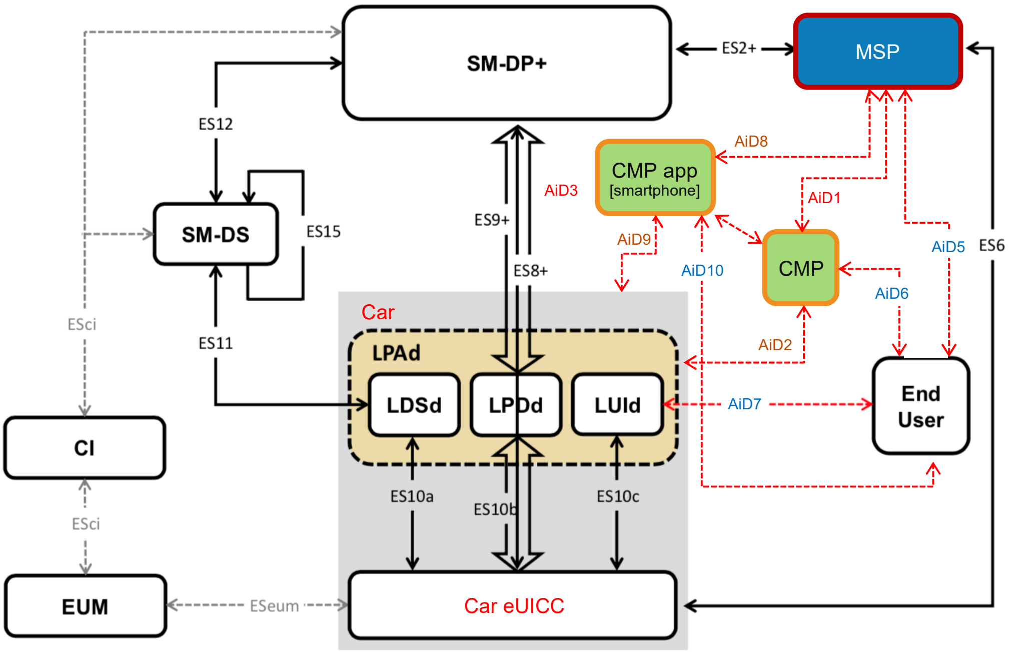
AiD9 (CMP app [smartphone] <-> CMP app [Car OS])

- Provision of Car details
- Provision of DownloadInfo
- Potential use of smartphone as an authenticator etc. (see section 5.2.1)

AiD10 (User <-> CMP app [smartphone])

- Onboarding the user to the AiD service and in-life service management (implementation specific user interface)

The following diagram illustrates how the AiD framework might align with the Remote SIM Provisioning (RSP) architecture [SGP.21/22]:



- AiD4: CMP app [Car OS] not shown
- AiD6: User <-> CMP or User <-> CMP app (not shown)
- Car performs LPA & LPM functions
- Car HMI and/or CMP app [Car OS] performs LUI function

Figure 12 AiD within context of RSP architecture

4.2 Category A: CMP <-> MSP account federation

In this category, a user's mobile subscription is linked to their CMP account during onboarding to the AiD service to enable a federated approach, the CMP being issued with a user-specific time-limited[16] token (MSP_token) that it can present to the MSP in subsequent B2B API calls[17]. The CMP backend retrieves the information needed by a Car (DownloadInfo) to instigate the mobile subscription provisioning process and bundles it with the AUP for download to the Car. The Car can then use this information (with explicit user authorisation[18]) for interfacing with the user's MSP to download and install an OP.

Example onboarding and Car provisioning flows for this Category are as follows:

Onboarding:

1. User registers to the CMP via a CMP touchpoint (e.g. online portal or app) and creates their AiD User Profile [AiD6]
2. User redirected to their MSP to authenticate and authorise usage of their mobile subscription with the AiD service [AiD5]
3. MSP issues MSP_token to CMP for use in API calls~~;~~[19] [AiD1]

Car provisioning:

1. User authenticates to their CMP a/c in a new Car via the CMP app in the Car [AiD7; AiD2]
2. CMP checks current service eligibility status with the MSP, and if eligible, proceeds to request DownloadInfo from the MSP, also passing Car details so that the OP can be tied to the Car eUICC (EID), and the MSP has the Car details where needed for Car & eUICC eligibility check information, billing & customer care purposes [AiD1]
3. CMP delivers AUP + DownloadInfo to the Car [AiD2]
4. Car uses the DownloadInfo to instigate the process of provisioning an OP into the Car eUICC [AiD3]
5. Once installed, the OP is linked to the AUP in the Car
6. Car sets up a local authentication method with the user for enabling their AiD service (AUP and OP) on Car-entry going forward – more discussion on potential authentication options in section 5.2.1

[16] Security policies typically require a time-limited token. The time period may be large to limit friction in the user journey (e.g., ~month)

[17] i.e., essentially the user authorises the MSP to delegate authority to the CMP for requesting the DownloadInfo on the user's behalf; the user then instigates the provisioning of their mobile subscription for the intended Car

[18] captured via the Car on-the-fly or potentially pre-cached depending on MSP policy. SGP.21/22 requires explicit user intent hence pre-caching is not available in the specification. The aforementioned enhancements may be discussed in future to allow for an improved user journey.

[19] The basic feature linked with the AUP is the mobile subscription for telephony and data connectivity. In an extended use case the MSP also may provide VAS metadata to CMP for inclusion in the AUP

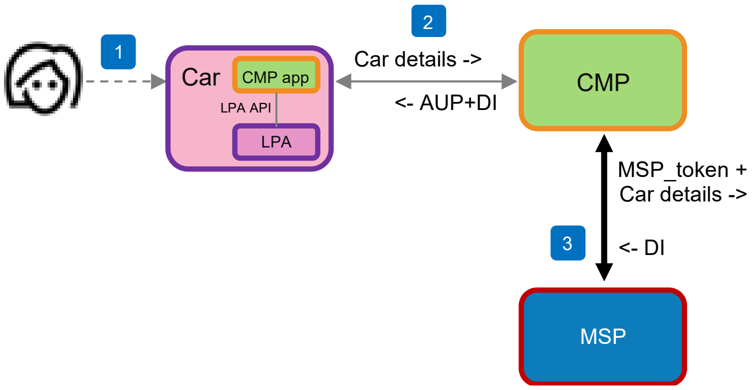


Figure 13 Category A: Car provisioning via CMP backend

General comments:

- Category A is designed to provide a smooth user experience and allow for a very high degree of automation with different users using a single Car, or a single user accessing multiple Cars
- Car provisioning user experience: user authenticates at Car-entry and provides confirmation, if requested, via the Car HMI to provision a new Car with their AiD service
- AUP + DownloadInfo bundled and delivered to the Car via a single mechanism
- Smartphone can be used to step-up authentication robustness and obtain user authorisation where required (e.g., via SMS OTP or SIM-based authentication)
- Option of using existing TS.43 ODSA infrastructure if available (with modifications) or separate RESTful APIs for the CMP backend to obtain the DownloadInfo from the MSP [AiD1]
- A key consideration is ensuring adequate trust and security between the MSP and CMP such that the CMP can act on the user’s behalf in this way. Section 5.2 provides more discussion on security & risk considerations.
- The authentication against the AUP in a given Car is used as a mechanism to trigger the provisioning of the AiD service. This may include the provisioning of the user’s OP into the Car.
- A user’s mobile subscription and AUP are linked within the AiD service such that whenever the user authenticates to the AiD service in a new Car supported by their CMP, their AiD service (e.g., AUP and an OP for their mobile subscription) is seamlessly provisioned into that new Car
- The ability to scale the AiD service to accommodate more CMPs and MSPs and the ability to easily update and evolve the AiD framework will be dependent on a common interface being deployed between CMP and MSP

4.3 Category B: Smartphone centric

In Category B, the solution is orientated around use of a CMP app downloaded to the user’s smartphone for both onboarding to the AiD service and initiating the Car provisioning process. Such an app may also be used within the operation of the AiD service as mentioned previously.

Onboarding example flow:

1. User downloads CMP app to their smartphone
2. User registers/logs in[20] to the CMP via the app and creates their AiD User Profile [AiD6]
3. User connects with their MSP to authenticate (e.g., via WebView in CMP app or using EAP-AKA which would provide a smoother user journey) and authorise usage of their mobile subscription with the AiD service [AiD5]
4. MSP may provide VAS metadata to CMP for inclusion in the user's AUP (as appropriate) [AiD1]

Three topology options are described within Category B that address the availability of interfaces between the different elements of the architecture:

- Topology B1 depicts a Car provisioning use case based on the availability of a Car-Smartphone interface (e.g. Bluetooth or NFC) and a Car-CMP interface (e.g. 3GPP connectivity)

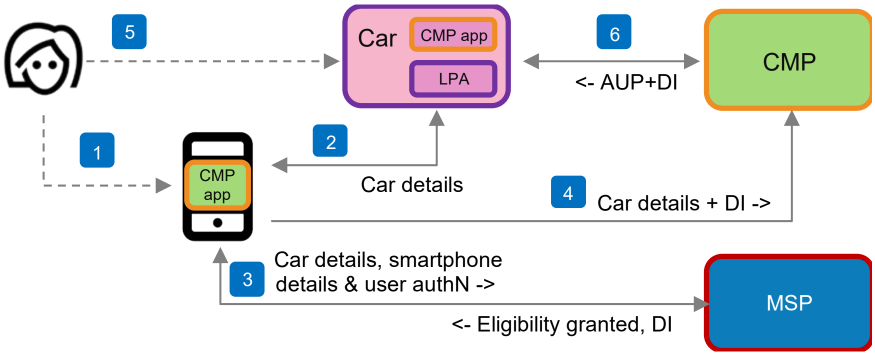

5
Car
CMP app
LPA
6
<- AUP+DI
CMP
1
CMP app
2
Car details
4
Car details + DI ->
3
Car details, smartphone details & user authN ->
<- Eligibility granted, DI
MSP

Figure 14 Topology B1: Car provisioning with DownloadInfo bundled with AUP with smartphone/Car and Car/CMP interfaces

[20] User can log in if already pre-registered to the CMP, e.g., via the CMP's online portal

- Topology B2 depicts a Car provisioning use case based on the availability of a Car-Smartphone interface (e.g. Bluetooth or NFC) – no direct Car-CMP interface required for the provisioning process

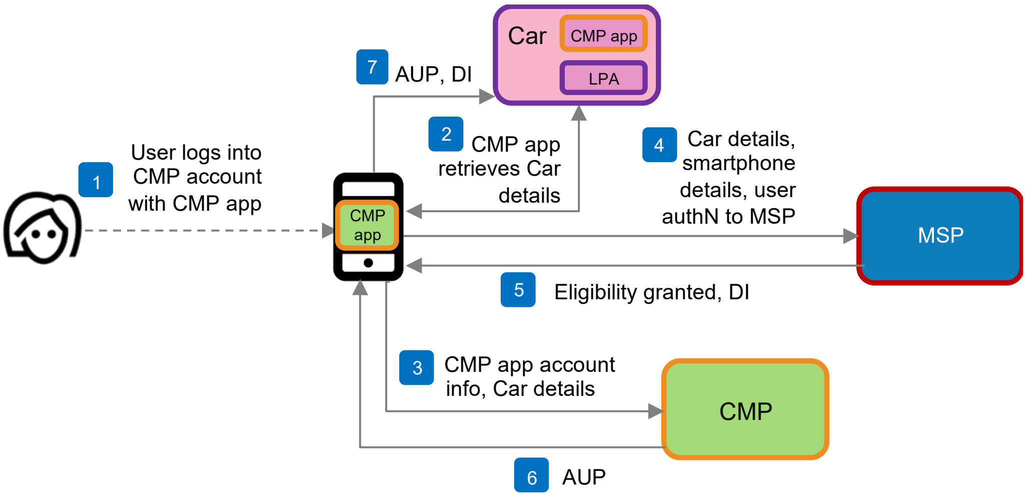

Car
CMP app
LPA
7 AUP, DI
2 CMP app retrieves Car details
4 Car details, smartphone details, user authN to MSP
1 User logs into CMP account with CMP app
CMP app
MSP
5 Eligibility granted, DI
3 CMP app account info, Car details
CMP
6 AUP

Figure 15 Topology B2: Car provisioning with DownloadInfo bundled with AUP and delivered over smartphone/Car interface

- Topology B3 depicts a Car provisioning use case, based on the availability of a Car-CMP interface (e.g. 3GPP connectivity) – no direct Car-Smartphone interface required

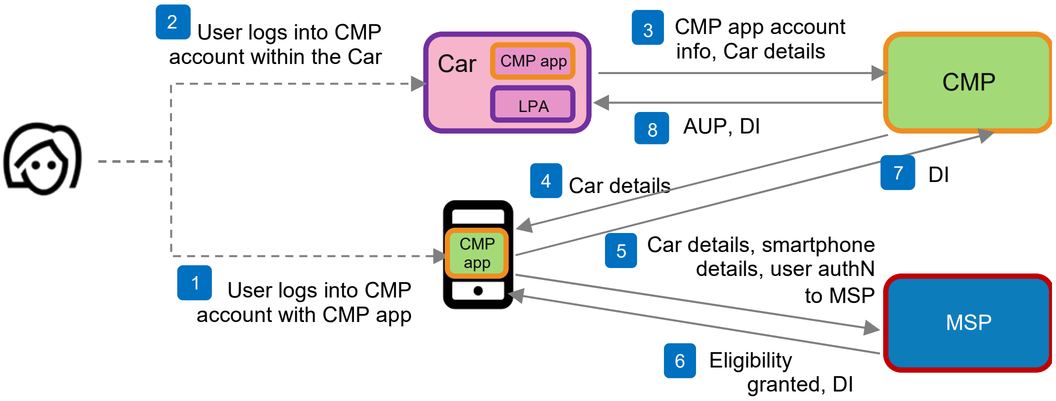

2 User logs into CMP account within the Car
Car
CMP app
LPA
3 CMP app account info, Car details
CMP
8 AUP, DI
4 Car details
7 DI
CMP app
5 Car details, smartphone details, user authN to MSP
1 User logs into CMP account with CMP app
MSP
6 Eligibility granted, DI

Figure 16 Topology B3: Car provisioning with DownloadInfo bundled with AUP and delivered over Car/CMP interface

An example provisioning flow for Topology B3 is as follows:

1. User unlocks the CMP app resident on their smartphone (and in doing so authenticates to the CMP and the AiD service) [AiD6]
2. User authenticates in the Car to their CMP
3. Car provides the Car Details to the CMP
4. CMP app receives the Car Details from the CMP

5. User authenticates (via the CMP app) to their MSP and instigates a request to add the Car to their mobile subscription[21] [AiD8]
6. User notified that request has been granted and the OP is ready – CMP app fetches the DownloadInfo from the MSP
7. CMP app passes the DownloadInfo on to the CMP
8. Car obtains the user's AUP and the DownloadInfo from the CMP (note: other implementation options are also possible[22])
9. Car uses the received DownloadInfo to instigate the process of provisioning an OP into the Car eUICC
10. Once installed, the OP is linked to the AUP in the Car
11. Car sets up a local authentication method with the user for enabling their AiD service (AUP and OP) on Car-entry going forward

General comments:

- Category B is a Smartphone centric approach that is fully compliant with existing standards such as SGP.21/.22 and TS.43
- The smartphone is a key component necessary for initiating download of the mobile subscription to a Car. Through the CMP app on the smartphone, the CMP is able to interact with the user and provide them with a comprehensive set of functionality for managing their AiD service both within and away from the Car
- The user may interact directly with the MSP to trigger OP download
- The smartphone app can access phone capabilities directly to perform eligibility checks and facilitate support of multidevice Car+smartphone services
- Car capability info can be relayed via the smartphone app to the MSP for an eligibility check of the Car and its eUICC
- The authentication against the AUP is used as a mechanism to trigger the provisioning of the AiD services. This may include access to the user's mobile subscription if it has been provisioned via the manual Car provisioning process
- The usage of a mobile subscription across cars is configured by the user
- Scalability and updateability is dependent on the implementation efforts for the CMP App on different Smartphone OS and the interface between CMP App and MSP backend

[21] the app passing the Car details retrieved from the Car so that the OP can be tied to the Car eUICC (EID) and the MSP has the Car details for billing & customer care purposes where needed. The smartphone app can also pass details of the smartphone where needed to support eligibility checks for multi-device services.

[22] e.g., the Car polls the SM-DS or the smartphone provides the DownloadInfo direct to the Car over Bluetooth etc.

5 Additional considerations

In addition to the functional requirements outlined and discussed in sections 3 & 4, this section discusses some of the additional requirements and considerations relating to data handling, privacy, and security & risk.

5.1 Data handling & privacy considerations

As part of the onboarding flow, information about the user may need to be shared by the MSP with the CMP to support set up of the AiD service and generation of the AiD User Profile. Likewise, the CMP may need to share information back to the MSP on the Car(s) that have been provisioned against the user's mobile subscription so that the MSP can provide itemised billing and customer care to its customers.

In such interactions, user privacy should be protected and minimal disclosure of user personal information should be practised wherever possible in addition to ensuring GDPR compliance and abiding by all other local regulations at point of implementation.

Based on the user stories, the following information might need to be known by each actor:

	MSISDN	AiD service subscription	User information[23]	# OPs/cars provisioned	Car details per OP	Current enabled OP/Car	OP usage records
User	Y	Y	Y	Y	Y	Y	Y
MSP	Y	Y	Y (CRM)	Y	Y[24]	Y	Y
CMP	TBD[25]	Y	TBD	Y	Y	Y[26]	N

Table 5 Privacy: information known to each actor

- MSP will have visibility of the cars that have been provisioned against the user's mobile subscription + usage per Car
- CMP will need to provide Car details to the MSP to enable the MSP to identify each of the cars that are linked to the user's subscription for use in their communications with the user
- CMP will have visibility of which cars the user has linked to their AiD User Profile and may have visibility of which mobile subscription they relate to
- User will be able to see via their CMP or MSP accounts which cars are linked to their mobile subscription(s)

[23] e.g., name, address, nature of mobile subscription (personal/business) etc.

[24] Needed for itemised billing and customer care purposes

[25] For user notification in the Car and customer care purposes the user's MSISDN may need to be known to the CMP/Car, or a registration token may be used instead of MSISDN

[26] Will know implicitly by the user logging in to their AiD User Profile in a particular Car

5.2 Security & risk considerations

5.2.1 User authentication & authorisation for Car provisioning

An important requirement within the AiD framework is in ensuring that the user is properly authenticated and provides their authorisation when provisioning a new Car with an OP for the user's mobile subscription and also that the user is properly authenticated on Car-entry to ensure that only the rightful owner has access to the OP within the Car.

The MSP may require different levels of assurance depending on the context; for instance, an MSP may enact a policy whereby:

- Enabling an AiD User Profile (and associated OP) requires a single factor of authentication
- Installing an AiD User Profile (and associated OP) in a new Car requires two (or more) factors of authentication, and perhaps one that is SIM-based

Authentication may be performed by the CMP, the MSP or both depending on the number of authentication factors used. The robustness of the authentication mechanism will be dependent on how and where the authentication and authorisation takes place:

- The device through which the user authenticates and provides authorisation should ideally be the Car upon which the OP will be installed, hence avoiding any potential error or fraud where an OP is downloaded and installed in the wrong Car
- It may only be possible to support a single factor of authentication via the Car itself (e.g., username/password credentials or possession of a particular car key) in which case additional robustness may be obtained via the user's smartphone as a second factor of authentication; e.g., via issuance of an SMS One Time Password (OTP) received by the user via their smartphone that the user is required to enter via the Car or CMP smartphone app
- The smartphone itself can also be used as a possession factor and as an authenticator with the user authenticating via the smartphone using credentials or a biometric (e.g., via FIDO2 CTAP):

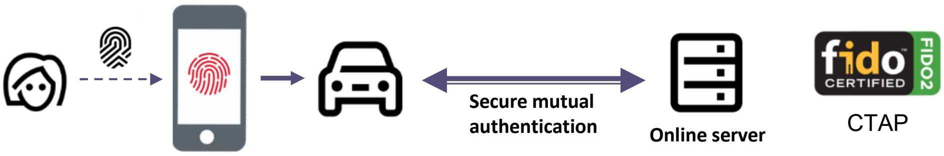


Figure 17 User authentication via FIDO2 CTAP

User authentication and authorisation when provisioning a new Car with a user's AiD service may be achieved via measures such as the following:

1. User authenticates to the CMP when entering a new Car
2. User provides confirmation (yes/no) prior to the Car initiating the OP download process

3. MSP prompts the user to confirm OP download by entering a OTP or authenticating via their smartphone, or perhaps entering a Confirmation Code as defined in SGP.21/22
4. Once the OP has been downloaded and installed, further confirmation can be sought from the user prior to enabling the profile (yes/no)
5. MSP can notify the user (e.g., via SMS) that their mobile subscription is now being used in a new Car; if this was in error (or due to fraud) the user can then take action

In practise, the best user experience when provisioning a new Car might be obtained by using steps 1, 2+3 combined and 5.

5.2.2 RSP Operational Profile provisioning: risk mitigation

The following risks have been identified and will need to be covered either through description of mechanisms to mitigate the risks or through specific implementation of the solution (non-exhaustive):

Compromised authentication to MSP

- Attack: Attacker phishes user for their MSP authentication credentials and thereby can bind the user’s mobile subscription to their own CMP user a/c
- Same situation as an attacker phishing a user for their authentication credentials and obtaining access to the user’s mobile subscription through requesting a new SIM => no different to current risk faced by MSPs

Compromised authentication to CMP

- Attack: Attacker phishes user for their CMP authentication credentials
- Whilst this would allow the attacker to gain access to the user’s AiD User Profile in the attacker’s own Car, downloading & installing an OP for the user’s mobile subscription could be protected through the use of an out-of-band authentication method between MSP and user
- The user would also receive a notification (including Car details as necessary) from their MSP that a new OP was now active against the user’s mobile subscription and hence could challenge if this was incorrect

Rogue CMP

- Attack: user tricked into binding their mobile subscription to a rogue CMP during onboarding
- MSP will only integrate with CMPs with whom they have an established commercial/legal contract
- MSP can utilise an out-of-band authentication to ensure that the user is aware of and authorising the OP download request
- User will also receive a notification from the MSP whenever a new OP has been activated against their mobile subscription and can challenge if necessary

CMP delivers DownloadInfo to wrong Car (CMP error)[27]

- CMP delivers AiD User Profile (and DownloadInfo) to the wrong Car (CMP error)
- Assuming the EID is passed to the MSP in the provisioning request, the OP will be bound to that specific EID hence avoiding the received DownloadInfo being used by the wrong eUICC
- In addition, User Simple Confirmation at the Car HMI should be declined by the user/owner of the Car => an out-of-band authentication method would help to strengthen robustness

[27] Category A and possibly Category B depending on implementation

Annex A Additional details

A.1 Candidate future ideas & potential requirements

Support for changing CMP

A potential future need is for users to be able to choose which CMP they would like to use for their AiD service (whilst respecting the principle of only 1 CMP per Car). In order to facilitate this capability, it might be useful to define a common schema to allow the user to port their AiD User Profile between CMPs.

Support for remote removal of RSP OP

As noted in section 3.5, there may be a need to remove an OP from a Car remotely – for instance in the scenario of a Car Rental company. Ongoing work in RSP standardisation on remote profile management (RPM) may provide a set of remote operations that could be used within the AiD framework for managing lifecycle events.

Value Added Services

MSP may provide the user with other Value-added services (VAS) to be used within the AiD service.

Simultaneous support of a user's AiD service across more than one Car at a time

Within this document, it has been assumed that a user would only be accessing their AiD service in Cars 'one at a time'. However, there may be scenarios in which the user may want/need to have their AiD service active in more than one Car at a time, hence these scenarios will need further study.

Ability to pre-provision a Car

Whilst this document discusses the scenario in which the Car is provisioned by the user at the point at which the user wishes to use the Car, there may also be scenarios in which it would be beneficial to provision a particular Car with the user's AiD service prior to the user having access to the Car – for instance, in a Car Rental scenario.

Corporate use cases

There are a number of commercial opportunities for using the AiD service in a Corporate setting ranging from simple company car usage through to management of a fleet of vehicles and ensuring personal connectivity for the individuals allocated to those vehicles (e.g., in the case of emergency services/first responders).

A vehicle may be allocated to a single user (e.g., company car) or be accessible to multiple employees with policy management being used at the CMP (fleet manager) to control which users are allowed to use their AiD User Profile and mobile subscription within a particular vehicle.

In the case of a company car, it may need to be provisioned with both personal and business mobile subscriptions.

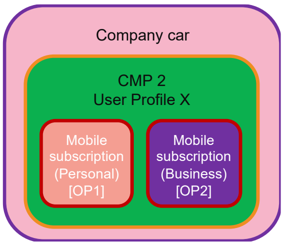

Company car
CMP 2
User Profile X
Mobile subscription (Personal) [OP1]
Mobile subscription (Business) [OP2]

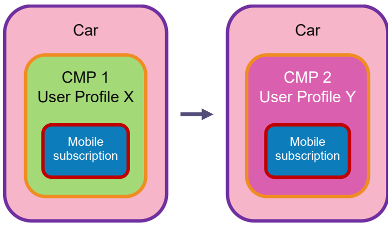
Figure 18 Single AUP: multiple mobile subscriptions

For example:

- User links their personal mobile subscription to their corporate CMP account
- Fleet manager can control whether or not a user is allowed to link their personal mobile subscription to their corporate CMP account and also whether the user is allowed to download their corporate AiD User Profile (and associated OP) to a particular corporate vehicle
- Once installed, user is able to toggle between their OPs (personal, business) via the AiD function in the Car (only one OP can be in use at a time; i.e., Dual-SIM; Dual Standby)
- Requires support in the Car eUICC for two enabled OPs (may be delivered through future RSP standardised features or via the implementation of several eUICCs) and an ability to manage which OPs are enabled

<ins>Open CMP <-> CMP app [Car OS] interface (AiD2)</ins>

- Ideally the CMP app [Car OS] <-> CMP interface should be open to ensure that a range of use cases and business models can be supported, such as a Car Rental company managing cars from different Auto OEMs or a car owner switching between CMPs based on the services they offer
- User downloads CMP app of their preferred CMP and installs in the Car OS
- Generic enablers/interfaces exposed by the Car to the CMP app and/or to the CMP back-end



Example of user choosing to switch CMP (but needing to generate a new user account with the new CMP)

Figure 19 User choice of CMP

A.2 Signal attenuation issues in-car

A key driver for the definition and deployment of the AiD service is to mitigate some of the issues experienced today in using a smartphone as a modem within a car by deploying dedicated infrastructure within the car and provisioning the eUICC with a user's mobile subscription. This section explains those issues.

Smartphones are often used in cars for providing telephony, content services and data connectivity, either through tethering the phone to the car via USB or pairing it to the car HMI over Bluetooth. Such an approach, whilst convenient, is often not reliable due to the signal attenuation resulting from operating the smartphone as a modem for providing connectivity within the metal chassis of the car.

The amount of signal loss varies based on a number of factors, such as the car material, the number & size of the windows, and the positioning of the smartphone in the car. In the best case, with the smartphone placed on the dashboard (e.g., in a cradle[28]), the signal loss is of the order of 6-8dB[29] which can result in a complete loss of service if travelling through areas with already poor coverage.

Moving the smartphone to the console (the most common location) or leaving the smartphone in a bag in the footwell increases the signal loss to between 9-12dB and 13-18dB respectively, hence having a substantial impact on the robustness of the connection that the smartphone is able to provide[30]. It is expected that this issue is likely to get worse as cars evolve to provide a more comfortable environment and increase shielding in accordance with regulation.

Some handsets now have 4 receivers to better receive the signal in situations of deep indoor propagation such as in the car, but the issue still remains and especially so in the uplink. An additional consideration is whether in-car transceivers will be able to support all the required bands (of all MSPs).

[28] e.g., if used as a satnav or for calls in those cars that don't have integrated capabilities

[29] In-car Mobile Signal Attenuation Measurements, Ofcom UK, https://www.ofcom.org.uk/__data/assets/pdf_file/0019/108127/in-car-mobile-signal-attenuation-report.pdf

[30] TR 38.901 makes assumptions on the car penetration loss: 9db and 20dB without and with metalized car windows respectively and a standard deviation of 5dB, see section 7.4.3.2

Annex B Document Management

B.1 Document History

Version	Date	Brief Description of Change	Approval Authority
1.0	3/6/21	Approved by TG May/June 2021	TG

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsma.com

Your comments or suggestions & questions are always welcome.