# What is the PCR?

#### Common usage

# Pseudonymous Customer Reference, or PCR, is an identifier of an end user issued by an operator Identity Gateway (IDGW) to a Service Provider (SP). PCR is used by Mobile Connect to reference uniquely a pairing between a specific end-user and a specific application/web service, inside the specific operator perimeter. In other words, PCR is basically unique for the tuple {specific operator, specific end-user, and specific application/web service}. SP MUST NOT consider PCR globally but only within the perimeter of the issuer operator.

The PCR will be found in id\_tokens in the field “sub” as described in OpenID Connect 1.0 (<https://openid.net/specs/openid-connect-core-1_0.html#IDToken>). As stated in the pointed specification, the PCR is a locally unique for the End-User within the Issuer perimeter and never reassigned . This property MUST be guaranteed by the issuer operator.

# As a definition, end user is the effective user of the MSISDN and not some other people which may have a link with this MSISDN (notably in business to business or household context: contract owner, company, payer ...). This is an important notion especially while some attributes will be consumed by SPs and will be linked to the PCR on SP side.

#### Format

The format of the PCR is up to the operator. It must be unique within the issuer operator perimeter. As an example, it could be generated as a GUID (Globally Unique Identifier), 5 groups of 32 hexadecimal (base 16) digits, separated by hyphens.

4567e123-e89b-12d3-456a-426655440000

It is important to note that the same PCR could be found for 2 distinct issuers. In this case, they are referencing distinct users. **This is the reason why it is crucial that SP always consider PCR associated with the related issuer.**

#### Delivery

# The PCR is delivered to the specific application/web service by the operator Identity Gateway (IDGW) after a successful end-user's authentication and is contained in the ID Token returned in the Open ID Connect response. This is the field “sub” (subject\_id).

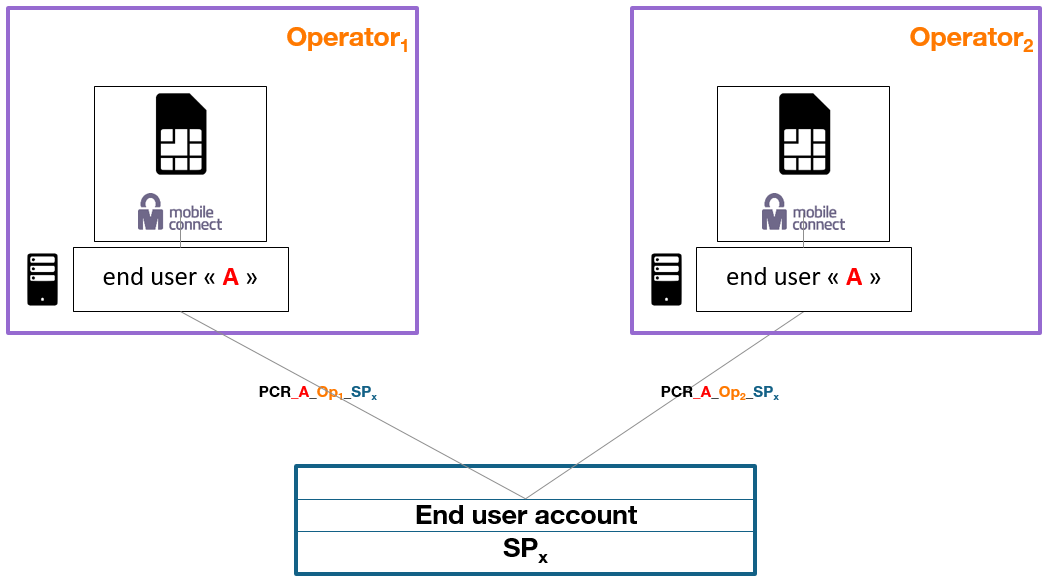
# 

# Why use the PCR?

By using the PCR, there is no requirement to provide personal data about the user for access to an application/web service. The service provider (application/web service) is assured that an actual user has authenticated using Mobile Connect and applications can then request additional information about users with their permission. This allows users to be confident their personal information will only be shared with the applications they choose with their explicit consent.

The application/web service stores the PCR got from a specific operator against the user account in their federation database.

Note that end user could have 2 MSISDNs, each from different operator, leading to the storage of 2 PCRs.



# PCR lifecycle

PCR is generated by the operator at the first authentication of the end user requested by the SP.

As defined, PCR is linked with operator, end user and application/web service. It means that PCR lifecycle is not directly correlated with MSISDN lifecycle. As a consequence:

* If a user switches of MSISDN, the operator may keep the same PCR towards the third party.
* If the MSISDN is not anymore allocated to the end user for any reason (end of contract, same contract owner but new end user…), link between end user and MSISDN must be deleted. In the same time, the PCR may still exist and is still be attached to the end user. The PCR can be used later, for the same end user, with a further MSISDN or with others MSISDNs.

There is an indirect link between PCR and MSISDN as MSISDN is the basis of Mobile Connect Sim Applet / SAA used as authenticator in Mobile Connect ecosystem.

Depending on operator’s policies, end user can also request to renew or delete PCR to be used to a specific Service Provider.

# Is the PCR secure?

The PCR is unique to each application/web service and user account combination inside an operator perimeter. Other Mobile Connect enabled service providers won’t be able to correlate PCRs in their database because they will receive different PCRs for the same end user (pairwise PCRs).

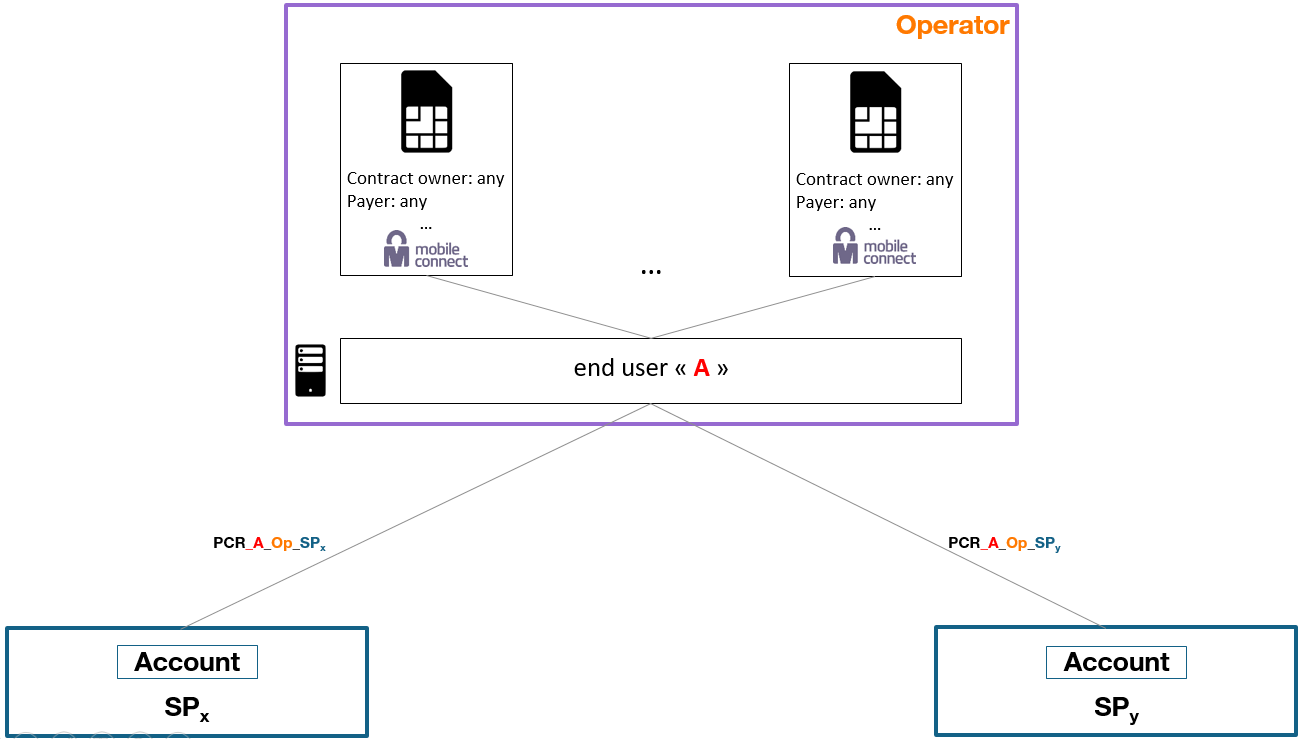
However, the operator IDGW will create the same PCR for a given end-user if the ’sector\_identifier\_uri’[[1]](#footnote-1) parameter is the same for a group of applications/web services. More specifically, a single service provider can have the same PCR for a user across all of their own applications/web services.

# PCR concept extension

#### Multi MSISDN

End user can have several MSISDNs in the same operator and PCR delivered to the third party can be the same based on operator rules and/or end user choices, whatever the MSISDN used for authentication is.

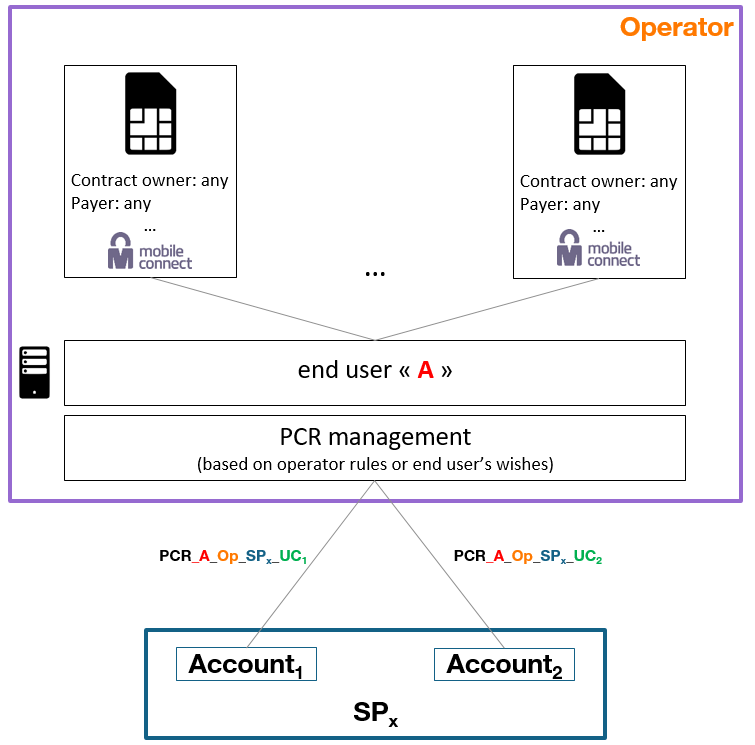
As reminder, PCR is linked to the person. It is not the case of the MSISDN which can be used or owned by another person. MSISDN is linked to the authenticator enabling to authenticate the person.



#### Multi PCR

The basic concept of PCR is: 1 PCR for the tuple {specific operator, specific end-user, and specific application/web service}. It is however possible to extend this concept to propose more services to end users based on use cases.

As an example for an “ads” service provider, an end user could wish to use 2 accounts: “fake one” to ask questions to seller and “official one” to buy when decision is taken, this without enabling the service provider to link both accounts. During authentication phase and based on which account the end user wants to use, it could be proposed to him to select which PCR (or alias in end user terminology) he would like to use.



Note that this PCR selection could be also based on MSISDN used to authenticate.

1. 'sector\_identifier\_uri' is a mandatory parameter in the authorisation flow that contains all the URLs prescribed by the service provider (the application/web service owner) while creating the application or web service in the Developer Portal. The mandatory URL in the ’sector\_identifier\_uri’ parameter is a ‘Redirect URL’. It is aimed at ensuring all the responses from an IDGW are delivered to the correct service provider’s applications/web services. [↑](#footnote-ref-1)