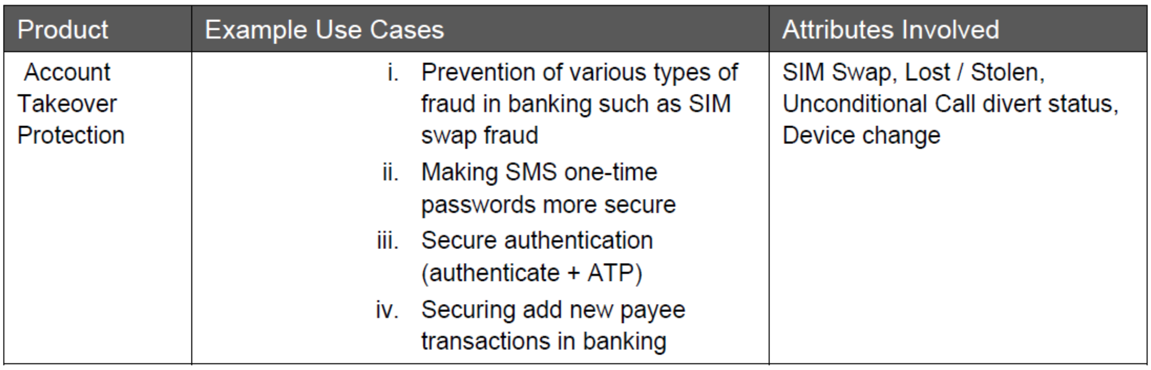
Account Takeover Protection (ATP) – SIM SWAP

ATP allows Service Providers to check attributes associated with a User's mobile account to provide a secure method of combatting identity fraud.

Many online banking accounts today are protected using secure online banking credentials (e.g., password and secret customer number), and additionally using the phone number associated with the User's bank account to increase security. This two-factor security helps mitigate fraud if one of the factors is compromised, for example if the User's online banking credentials have been stolen.

ATP allows SPs to perform additional checks on the User's mobile phone status to determine whether or not this factor may have been compromised. In particular, the service returns an indication of whether there has been a recent SIM swap and may optionally return other information relating to the User's mobile account:

Use case examples:



Product	Example Use Cases	Attributes Involved
Account Takeover Protection	i. Prevention of various types of fraud in banking such as SIM swap fraud ii. Making SMS one-time passwords more secure iii. Secure authentication (authenticate + ATP) iv. Securing add new payee transactions in banking	SIM Swap, Lost / Stolen, Unconditional Call divert status, Device change

The key aim of the ATP service is to flag to an SP whether the user's SIM has recently been changed which might indicate fraud where the attacker is attempting to circumvent an SP's second-factor authentication on a mobile device. Depending on Operator implementation, the service may also provide additional information such as whether the device has been reported lost or stolen, or whether the user's SIM has been swapped to a different mobile device.

Service flow:

i. The SP wishes to make an ATP service request for this User.

ii. If this is the first time that an ATP service request has been made for the User then it may be necessary to obtain the relevant Operator ID GW details (Provider Metadata) for this User using the API Exchange Discovery service. These details can then be stored for future use.

iii. If the SP has previously requested the service and has an unused and existing valid Access Token, then a Resource Request can be made directly to the applicable Resource Endpoint specified by the Operator.

iv. Otherwise a full API request (OIDC Authorization Request) is made to the Operator ID GW Authorization Server using the User's MSISDN or PCR as an identifier and specifying the ATP service using the scope parameter.

v. If the User has for some reason revoked consent, then the SP should not make the request until the User has given their consent again. Note that the User should have flexibility to block the SP, to revoke the already given consent and to request explicit transaction-based consent to protect the user's personal data.

vi. The Operator validates the request and confirms if the SP has registered for ATP in accordance with the Operator's ID GW policy. In the event of an error the request is terminated, and an error response is returned to the SP Server.

vii. Assuming the request is valid, the Operator processes the request and returns an ID Token (security token), an Access Token which is used to retrieve the requested attributes (as specified in this document) from the relevant Resource Endpoint.

viii. Optionally Operator ID GW seeks User consent for sharing the ATP information via the User's mobile device (Authentication Device). Note though that such transactional-based consent is not recommended for the ATP service – more discussion on the legal options for acquiring user consent can be found in specification section 3.1 and GSMA Regulatory considerations for processing personal data and attributes for Identity services.

ix. If consent is requested by the ID GW and not given, or the Operator has insufficient proof that user consent has been captured by the SP, then an error message should be generated and returned to the SP instead of the Tokens.

x. In Server-Initiated mode, the SP can retrieve the ID Token and Access Token in one of two ways depending on what is supported by the ID GW in the server-initiated mode: using notification where the Tokens are sent to the SP's specified Notification Endpoint or by the SP polling the ID GW Polling Endpoint until a full response is obtained. Further details are provided in the Server-Initiated OIDC Profile specification.

xi. Assuming the request was successful, the SP receives the ID Token and Access Token and then uses the Access Token to make a Resource Request to the applicable Resource Endpoint in order to obtain the requested information.

There are following parameters possible in ATP userInfo response:

- mode – possible values BOOLEAN, TIMESTAMP, RISK_INDICATOR, HASH.

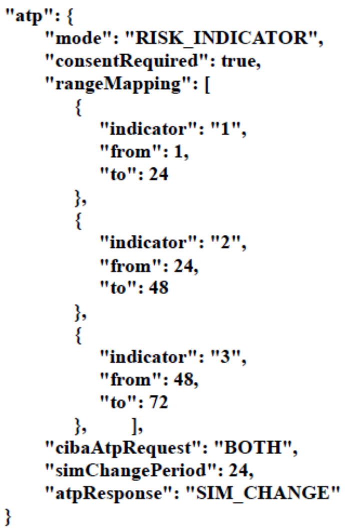
- consentRequired – specify if consent is required for mc_atp scope

- rangeMapping – defined ranges only for RISK_INDICATOR mode

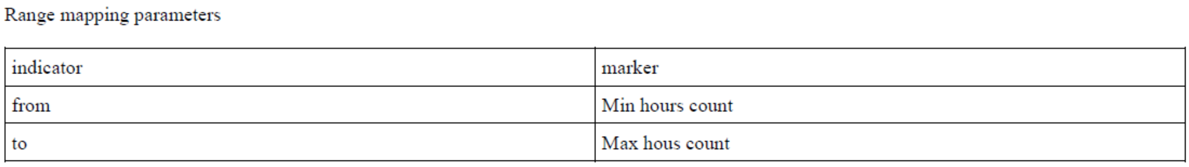
- cibaAtpRequest – defined Server Initiated Mode in which ATP is supported. Possible values: BOTH, NOTIFICATION, POLLING

- simChangePeriod – period in hours in which simChange is detected. This settings is applies only for simChange mode.

Example of “rangeMapping”



```
"atp": {
      "mode": "RISK_INDICATOR",
      "consentRequired": true,
      "rangeMapping": [
           {
              "indicator": "1",
              "from": 1,
              "to": 24
           },
           {
              "indicator": "2",
              "from": 24,
              "to": 48
           },
           {
              "indicator": "3",
              "from": 48,
              "to": 72
           },      ],
      "cibaAtpRequest": "BOTH",
      "simChangePeriod": 24,
      "atpResponse": "SIM_CHANGE"
}
```



Range mapping parameters

indicator	marker
from	Min hours count
to	Max hous count