May 31, 2018

Policy based Authentication Service with Mobile Connect

Bo Wang
Hewlett Packard Enterprise

Policy based Authentication Service with Mobile Connect

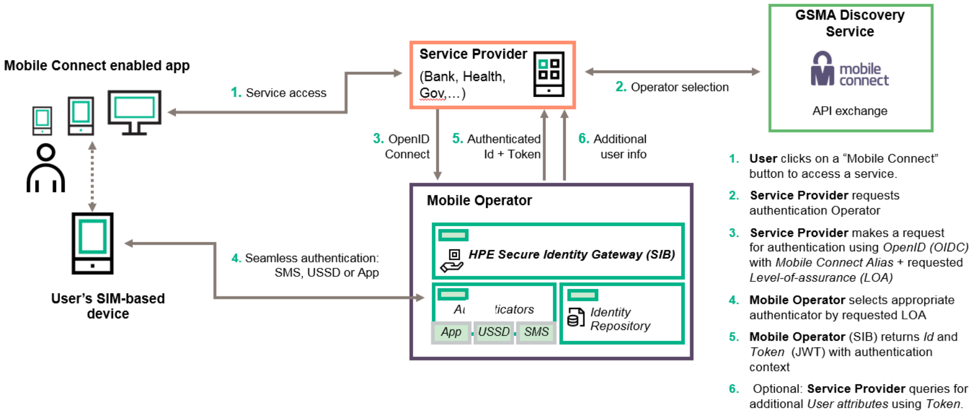
Abstract

Secure Identity Broker (SIB) solution provides authentication, authorization and identity services based on GSMA mobile connect standard and enables identity-focused services to carriers and Service Providers. We invent policy based identity services in SIB product to support variant customer requirements such as Delegation, Time Period control, Joint authentication, geographical location based authentication etc. Then differentiate our solution with vendors and maximize the customer value.

Problem statement

Nowadays, the mobile ecosystem, include users, MNO (Mobile Network Operator) and SP (Service Provider), become the most important part of Mobile Internet. However, up to this day, the online security of these services has shown a lack of performance in identity, security and privacy capabilities leading to the lack of trust from users. GSMA Mobile Connect [1] is proposed to address the issue. And new Secure Identity Broker [2] product is invested to provide authentication, authorization and identity services. For example, leverage mobile phone and fingerprint to authenticate to any 3rd party services which integrated with SIB. Figure 1 illustrates the GSMA Mobile Connect and SIB solution. Please note the service can be from different place from the user's mobile phone. For example, you can access your bank account from your laptop, while you ask logging, the authentication request will go to your mobile phone, which is registered as your mobile connect auth (Authentication/Authorization) device. There are multiple authenticators such SMS, USSD and Smartphone App (SAA) can be used to confirm the auth request.

However, while we discuss with CSPs (Communication Service Providers), we found there are challenges to support some advance use cases such as:



1. **User** clicks on a "Mobile Connect" button to access a service.
2. **Service Provider** requests authentication Operator
3. **Service Provider** makes a request for authentication using *OpenID (OIDC)* with *Mobile Connect Alias* + requested *Level-of-assurance (LOA)*
4. **Mobile Operator** selects appropriate authenticator by requested LOA
5. **Mobile Operator** (SIB) returns *Id* and *Token* (JWT) with authentication context
6. Optional: **Service Provider** queries for additional *User attributes* using *Token*.

Figure 1 Mobile Connect and SIB Solution

Parents want to know which services the children are using, and control the children's login for some sensitive service such as games. The control means the service login authentication will go to the parent's mobile phone, instead of children's phone, and also consider the time period and count, such as allow play Game X 2 times per day in weekend during 9:00 to 20:00 with parent's permit, and just reject (not bother parents) if out of the scope; but allow children login any education services logging with their own mobile phone; for a new service the child want to access, always let parent to check and authenticate to make sure it is suitable for children.

Multiple peoples' authentication for a high security service. The typical cases appeared in many movies: a safe box need 2 keys and each key is hold by one people, then the box can be opened only with the two peoples' agreement and presence.

Some services requires limit the serving location to be same as the user's location to avoid cheating or unexpected disturb for the user. For example, a bank ATM always allows the user to withdraw cash from ATM with his/her mobile phone in same place only; so if someone knows the user's phone number and try to initiate the withdraw request in a ATM, the request will be rejected silently and the bank may take his/her picture and send a warning.

Some user want to limit some service which can occur in specified place only. For example, a user may want his bank account can be accessed from his living city only, to minimize the potential risk.

Additionally, some service provider would like to let the user can see where is the serving location while he/she confirm the authentication request.

Our solution

We propose a solution to address those customer requirements with well-designed data model, mobile connect interface enhancement, internal flow and logic enhancement.

Figure 2 illustrates the enhanced data model in SIB to support the business cases. The key model "User/SP App Policy" defines the Policy on SP App (Service) for a user, and the Policy item is managed by the supervisor. The Policy item is described by a type and corresponding parameters. For case above, the following Policy type and parameters are described as table 1:

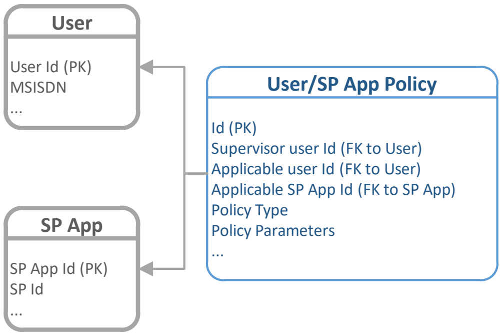


Figure 2 SIB Data Model Enhancement

Type	Description	Parameters	Examples
Delegation	Delegate auth request to the supervisor	N/A	Child (User 102) delegate service (SP App X)'s auth to Parent (User 101). One Policy can be defined here as Applicable user id is 102, supervisor user is 101, applicable SP app is X.
Time Period	Limit the time period can be used.	Linux crontable period definition	Child can play game Y in 9:00-20:00 weekend only. It can be defined as "* 9-20 * * 0,6". Parent is the supervisor to update the parameter.
Join	Join auth request	The user list need to be joined for the request	While user 101 auth service X, need join auth from user 102. User 100 is the supervisor. Then, applicable user is 101, parameter is 102, supervisor user is 100.
Colocation	The serving area should be same as the auth device	Maximum distance	Bank ATM service X need the auth device in 1 KM area of the ATM. Then applicable user Id is 0(all), SP app is X, Supervisor user is the bank SP admin user, parameter is 1000.
Location	The serving area should be limited as defined location	Point (Latitude + Longitude) and radius	User 101 wants limit bank account service Y can be used in home location 10KM only. Then applicable/supervisor user id is 101, SP app is Y, parameter is 4807.038,N; 01131.000,E; 10000
Block	Block the service to a specified user. A typical case is working with Join policy.	N/A	User 102 is blocked to use service X.

Table 1: SIB User/SP App Policy types

While a user initiated an authentication request to SIB, after validation the user internally and MNO externally, the applicable user of "User/SP App Policy" will be checked with current user. If no any Policy, following in normal case; otherwise need special logic to handle the Policies:

For Delegation Policy, the authentication request destination will be replaced by the supervisor, and a additional validation is required for the supervisor, if it is OK, the authentication request will be sent to the supervisor's auth device; after the supervisor confirm the request, the authentication code will be returned to the original user, and following to get tokens like normal process.

For Time Period Policy, current time will be checked with defined crontable, if it does not fall in the period, reject the request.

For Location Policy, SP need parse the serving location information from the original user request to SP and include it as an optional encrypted parameter in the redirect request to SIB, then SIB will calculate the distance with defined parameter to decide to continue or reject. Please note if location Policy is found but SP does not report serving location, the request will be rejected as well. The serving location information is an enhanced feature of SIB interface towards SP, which is not defined by GSMA Mobile Connect today.

For Colocation Policy, it requires Smartphone App authenticator (SAA) because it requires SAA to return the location of auth device (Smartphone), and then calculate distance with serving location which is reported by SP.

For Join Policy, SIB will handle the user list from Policy Parameter, for each user, SIB will validate the user internally and with MNO, then request the confirmation to their auth device one by one. If all join users are confirmed, then the original user can get the access code and continue to get token. Please note it should be used with Block policy usually. For example, service X need joined auth from user 101 and 102, but only 101 can initiated the request, then user 101 will have a Join policy, and 102 need a Block policy. If the joint auth can be initiated from both user 101 and 102, two Join policy need to be defined.

The supervisor can view and update the policy parameters in user portal after logging in. For the update relevant to other users, need the user to confirm the request with auth device.

Today, the supervisor and initial policy can only be created by SIB administrator on demand of user's request, afterward, the supervisor can manage owned policies.

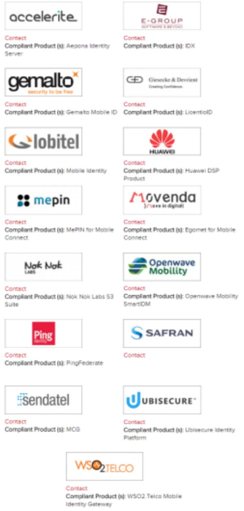
Evidence the solution works

The major changes of our solution are the business logic enhancement. Our current SIB flow implementation is FSM (Finite State Machine) [3] based and the transitions are implemented with Rule Chain configuration. We have evaluated the changes based on current SIB implementation and no any technical issues.

For Time Period, Colocation, Location and Block Policies, the flow is almost same, just need some additional steps to include the enhanced logic.

For Delegation Policy, the target user will be replaced to the supervisor, and the rest of logic is same.

For Join Policy, after current user's confirmation, an iteration logic is included to wait for confirmation from all other users, then continue with normal flow.



Contact
Compliant Product (s): Aepona Identity Server

Contact
Compliant Product (s): IDX

Contact
Compliant Product (s): Gemalto Mobile ID

Contact
Compliant Product (s): LicentioID

Contact
Compliant Product (s): Mobile Identity

Contact
Compliant Product (s): Huawei DSP Product

Contact
Compliant Product (s): MePIN for Mobile Connect

Contact
Compliant Product (s): Egomet for Mobile Connect

Contact
Compliant Product (s): Nok Nok Labs S3 Suite

Contact
Compliant Product (s): Openwave Mobility SmartIDM

Contact
Compliant Product (s): PingFederate

Contact

Contact
Compliant Product (s): MCG

Contact
Compliant Product (s): Ubisecure Identity Platform

Contact
Compliant Product (s): WSO2 Telco Mobile Identity Gateway

Figure 5 Mobile Connect Vendors in GSMA

Competitive approaches

Mobile Connect is a new solution, Figure 3 illustrates the vendors listed in GSMA, and some vendors provides only part of the solution. For example, MEPIN is our partner to provide the Smartphone App Authenticator. Although most of the vendors are small, but Huawei is also in the list. But anyway, as far as I know, no one can provide the features we described in this paper.

The policy based authentication feature differentiate our solution with vendors and maximum the customer value.

Current status

Today, our solution described in this paper has already been designed and evaluated.

Next steps

We will start the next release to include the new features described in this paper. Beside the policies we described above, some other policies, also can be added upon customer's new business requirement.

References

[1] https://www.gsma.com/identity/mobile-connect

Disclosed by Bo Wang – Hewlett Packard Enterprise