Becoming a Trusted Identity Provider: A blueprint for telecoms providers.

Introduction

Identity management sits at the heart of successful digital transformation. For businesses and service providers, it is the key to unlocking the triple goals of:

» Cost reduction derived from; comprehensive process redesign, customer journey reinvention, and service automation
» Revenue growth through higher customer retention and more effective marketing
» Competitive differentiation through world class customer experience and service underpinned by trust, security, and customer choice

The benefits of a strategic approach to identity management are not one-sided; they are mutual. For consumers and customers identity management provides:

» A convenient, frictionless online experience
» Knowledge that their privacy is being respected and protected
» A secure digital existence with personal data under their control

Headline grabbing news regarding data breaches resulting from cyber attacks and the misuse of data, even when legitimately acquired, continues to shine the spotlight on digital identity, raising important questions regarding not just how, but who should be responsible for identity protection.

For service providers, there is increasing anxiety regarding the threat and risk of getting it wrong. For consumers, there is rising awareness and momentum building for different approaches and more robust solutions to what is becoming the 'Trust Battleground'. In the Mobile EcoSystem Forum Global Consumer trust Report 2017, lack of trust was cited as the single most significant inhibitor to adoption of digital services and applications, with 88% of respondents saying they take positive action based on trust concerns; deleting apps, switching service providers, or leaving bad reviews.

Interestingly, the recent joint research paper from ForgeRock and Mycustomer, 'Building Customer Loyalty in the GDPR Era', shows clear evidence of strong correlation between ease of use and trust. If a service provider's customer journey and customer

experience are disjointed, overly complex, or repetitive, it leads to more than just frustration. As consumers become more savvy, their emotional reaction to a bad user experience is to assume that the service provider is incompetent, and therefore cannot be trusted to adequately take care of the basics around privacy, data protection, and security.

In this paper we set out the case for Communications Service Providers becoming trusted Identity Providers in their chosen markets. Providing 'Digital Identity as a Service' on behalf of consumers into a broad ecosystem of service providers eager to simultaneously accelerate and de-risk their digital transformation journeys is a compelling new business opportunity, capitalising on the rising awareness and concern regarding digital identity from both consumers and service providers alike.

We highlight a range of important market dynamics and considerations, suggest models for understanding the market opportunity, and provide technical design options and a blueprint for launch and evolution of Identity services.

Market Considerations

The idea of telecoms companies using their market position and large consumer base of customers to provide identity related services into other market segments is not new. The GSMA Mobile Connect concept (for which ForgeRock is a licenced vendor) is a good example of an industry wide initiative to provide entry level authentication services, based on a telco's ability to confirm data attributes such as name, address, phone number and email, and associate these to a secure device (a mobile phone) which can then be used to authenticate and authorise user interactions as well as provide, with consent, attributes to service providers.

Mobile Connect and Mobile Connect-like services have been launched in several markets around the world, including: Orange's 'Check and Go' service in France, MobileID across both Swisscom and Sunrise in Switzerland, and the T-Auth service in South Korea which has been adopted collaboratively by all the major mobile operators.

However the breadth and depth of service offerings, targeted market segments, technology solutions and value propositions adopted by telecoms operators around the world vary considerably, both within the GSMA Mobile Connect umbrella, and outside it where operators have developed bespoke solutions for solving specific issues within their market.

Consumer adoption, service provider adoption, practical market applications and commercial success have also varied considerably.

The key to understanding how a CSP can successfully position itself in the Identity market is to understand the value that it brings, both to consumers and to merchants and service providers.
In this section we examine some of the market dynamics that Operators should consider in their market analysis.

What Level of Assurance and Strength of Authentication Is Required?

Ensuring that a digital identity is 'authentic' poses two distinct challenges:

1. At the point of registration of an identity, how sure am I that the person registering it is legitimately who they claim to be? This is measured by 'Level of Assurance' (LOA).

1. At the point of using a previously registered digital identity, how sure am I that the person using the identity is actually the person who registered it? This is measured by 'Strength of Authentication'.

There are a number of considerations for telecoms companies when it comes to LOA. Firstly, the level of Assurance regarding telecoms customer records can vary considerably:

» For contract customers, typically the level of assurance is good because of the process required to provide banking details and proof of identity for credit purposes. The financial services companies involved are themselves subject to strong KYC regulations; therefore the data provided by them has a high level of assurance (typically LOA2). Even in the case of contract customers however the LOA process is not foolproof – the Customer (i.e. bill payer) to whom a SIM is registered may well not be the Consumer (i.e. User) of the SIM – if for example it has been handed off to a spouse, child, or other family member. This can increasingly create concerns in legislations where the identity of each user must be known and verifiable, e.g., for lawful intercept purposes.

» For prepaid customers, the level of assurance is generally very low or even non-existent. In some markets there are regulatory requirements to register a name and address even for prepaid SIM cards (e.g. Switzerland and Australia); however, many other markets have no such requirements, and pre-paid customers are effectively anonymous. Any data they provide is 'self certified' and would only qualify as LOA0.

» Similarly for enterprise customers, the level of assurance is low – companies may be obliged to inform the telecoms company of the name of the employee to whom a SIM has been assigned: however, this is rarely verified and does not come with an address or other identifying attributes.

Some use cases require very high levels of assurance, such as Banking KYC, where the primary value driver of an IDP is enhanced security. When telcos are not able to establish this, they should steer clear of these markets and use cases in their initial market strategy. In addition to variable LOA, where a telco's LOA is fundamentally based on data received from a bank, the value of providing this back to the banking industry may be limited, since it is a circular reference, unless the CSP is augmenting their data with additional information, such as real-time location data.

Where only lower LOA is available, Telecoms operators should focus on use cases where the primary value driver is convenience, (for example form filling and registration) rather than security (such as transaction authorisation and data protection) for third party services.

Setting aside LOA, when it comes to Strength of Authentication, mobile devices have great potential, due to their ability to deliver a wide range of different authentication methods via a range of different channels, all within a single device. Authentication methods include biometrics (fingerprints, facial recognition, etc), One Time Passwords via SMS and/or email, PIN codes to unlock the device, and secure on-device applications.

Competition vs Collaboration: Who Else Offers Trusted IDP Services?

The primary resource required to successfully launch a trusted IDP service is access to a large base of consumers and their basic identity-related data attributes (e.g. name, address, email, phone number, etc.) Telecommunications operators fit squarely into this category.

Access to consumers and their data is not sufficient by itself, but it is an essential prerequisite. Additionally consumers have to trust the organisation to respect their privacy and protect their data. In other words, they need to perceive that the organisation has a sound reputation, with high integrity, operational expertise, and technical competence in equal measure. Brand image and real competency in these core disciplines are key pillars for success.

In addition to telecoms operators, other types of organisations also have the potential to become Trusted IDP's, either in competition or collaboration with telecoms operators. These include governments, financial services organisations, (for example banks and credit Bureaux), social media companies, and online marketplaces. There are examples of both competitive and collaborative models emerging around the world. Here are a few examples:

» In Estonia, the Digital nation project allows anyone in the world to register for an Estonian government-issued digital identity (eResidency), with the primary objective of enabling people to establish and run a global business from within the EU.

» A number of European governments (e.g. Belgium, Germany, Italy) have launched eID schemes, which in turn have created opportunities for other organisations and consortia to leverage the high level of assurance associated with eID to launch a range of innovative consumer ID services. In Belgium for example, four leading banks and three leading mobile phone operators have formed a consortium called Belgian Mobile iD, and launched a service called 'itsme'. The service ties together a Belgian Government issued eID to a specific SIM card and PIN code combination to enable a mobile device to be used to authenticate a

user to, for example, confirm payments, place orders, and sign documents.

» In the UK, the GOV.UK Verify programme enables people to establish their identity online via a choice of 7 authentication partners, and this ID can then be used to authenticate the user into a wide variety of government services.

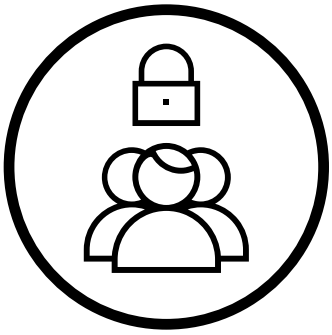
» In the UAE, the Emirates identity Authority, working in collaboration with government ministries, agencies, and commercial organisations (including banks and telecoms companies) has successfully extended the government digital identity scheme. Initially established for only border control, the scheme extends into a range of day-to-day commercial and civic applications. Biometrics are used for authentication, replacing the need to use passwords and PIN numbers.

» In Germany, two competing consortia have launched similar competing online identity schemes. Deutsche Bank initially partnered with: insurance company Allianz, publisher Axel Springer, car manufacturer Daimler, and online banker Postbank. They have subsequently been joined by Deutsche Telekom and Lufthansa to launch the 'Verime' Digital ID service. Similarly, media companies RTL Group and ProSiebenSat.1 Media SE have formed an alliance with United Internet and the online retailer Zalando.

» Social media companies including Facebook, Linked-in, and Twitter enable app and web-site developers to use their stored profile credentials and attributes as a convenient way to register and log-in, without the need for time-consuming repetitive typing of personal details.

» Online market places such as Amazon enable their unique customer identity to authenticate access across their myriad of retailers and traders connected to the marketplace in order to facilitate a secure and frictionless user experience.

What is particularly interesting about most examples of successful Digital Identity projects is the theme of an ecosystem or online marketplace encouraging collaborative approaches between a number of different organisations across a broad range of sectors to standardise an ID service. In addition to securing the broadest possible base of consumers, this ecosystem approach also delivers s broader range of useful data attributes into the identity system. It pulls data from different service providers, combining and sharing these (based on user consent). This gives rise to new and innovative services and richer insights into behaviour and consumer preferences.



Eric Ahlm, Research Director at Gartner, sums up the main driver behind this phenomenon:

"Risk management is no longer the domain of a single enterprise and it must be considered at ecosystem level. The success of my product or service is now fundamentally intertwined with others. My risk is their risk. Their risk is my risk. It's one in the same."

What Market Coverage to Offer?

This brings us to the final major market consideration when telecoms providers consider how to enter the Digital Identity Provider market: What market should we serve?

In the examples above, the 'potential target market' ranges from the global perspective of 'everyone in the world' for social media companies like Facebook, to a geographic market based on 'everyone in my country' for the likes of Belgian Mobile ID. Others define the market by commercial lines. This ranges from a shared customer base in the case of the German Media led consortia to an ecosystem of business partners in the case of Amazon to organisations within a particular industry in the case of GOV.UK Verify.

Whatever target market is selected, success will depend on a CSP's ability to offer full market coverage. As expectations of consented sharing of identity data increase, and indeed become legislated, the ability to do so across the market (ecosystem) participants becomes essential. Consented sharing equals increased trust and improved data quality, providing benefits for all market place participants. This is important for organisations that might benefit from using the IDP service to authenticate their customers. There is limited benefit, for example, from a Telco offering a stand-alone trusted IDP service to the insurance sector in their geographic territory, unless they command a very high market share. Typically in a competitive telecoms market, one player might command 20-25% of the market; however, this is not

sufficient to be attractive to insurance companies. They need at least 70-80% market coverage to make investment in the service worthwhile, which implies the need for Telecoms providers to join forces and offer a common solution, as was the case with T-Auth in Korea for example.

In the next section, we consider how these market considerations can help build a model that is both successful for the market and technologically appropriate.

Deciding on Market and Technology Strategies

Market Strategy

Deciding on your market strategy includes knowing what type of identity services you should offer, to what type of service providers, and for what segments of the market. This requires understanding of your identity capabilities in two dimensions:

1. What level of assurance do you have on your customer's identity? How certain are you of the authenticity of the customer identity and the identity attribute information that you hold? Typically this will be relatively strong for post-paid contract customers where KYC checks have been carried out as part of the contract process. However, parts of your customer base may not have very strong levels of assurance, such as pre-paid, SIM only, and business users within a corporate account. Even for contract customers, remember that the user of the device may not be the same person who is paying the monthly bill.

1. How strong are your authentication capabilities? This covers the range of techniques at your disposal for authenticating a user against the identity credentials that have been assured. This may be simply using the login capabilities of the device being used, or may be augmented by other authentication factors such as One-Time-Passwords, biometrics and push authentication SMS messages.

The following diagram shows how these two considerations combine to enable distinct market strategies, illustrated with examples of typical use cases and industries served. Where capabilities are limited in either or both dimensions (indicated in yellow), a market strategy based on a service that provides ***convenience to the consumer*** is viable. Where capabilities are well developed in both dimensions, market additional strategies based on ***protection*** of both the ***consumer*** and the ***service provider*** are also viable.

/LEVELS OF ASSURANCE

Self Assured: I assert who I am. Typically email confirmation and in this case the addition of the phone number and a check via SMS

Externally Assured: My self assertion is validated by an external trusted data source. Typically the addition of an address verification such as a credit card validation.

Externally Assured to a high level: My self assertion is validated by multiple external trusted data sources. This will vary from territory to territory but on top of credit card validation, additional sources such as national ID documents, utility bills, etc. are validated by an external service (E-KYC, for example); during this process it is also possible to add other concepts such as biometrics.

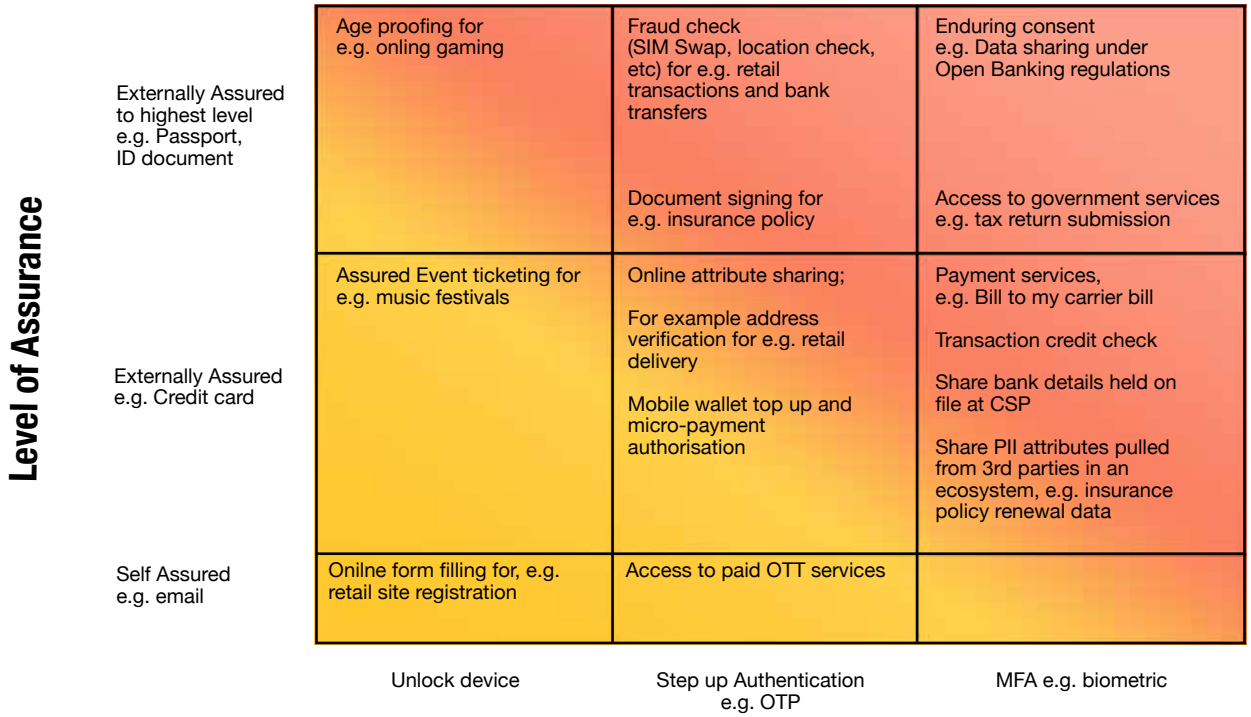
OIX report on Levels of Assurance

/STRENGTH OF AUTHENTICATION

My phone: When I have my phone with me, it is a good indicator that I am who I say I am.

Step up Authentication: I am trying to do something that requires a bit more confidence that I am who I say I am, so I am asked to enter my password of pin (or use the device's additional security technologies e.g. Face ID, Touch ID) to buy something, access more private information, or share some more important data.

Strong Authentication: I am trying to do something that requires even more confidence that I am who I say I am. So I am asked not only to enter my password or pin (or use the device's security technologies such as Face ID or Touch ID) but also use a strong authentication technology such as FIDO compliant Biometrics.



Technology Strategy

The primary consideration for a relevant technology strategy concerns how and where data is stored. In essence, should data be stored and retrieved from a central repository, or once verified, should it be distributed, including being stored in the device layer?

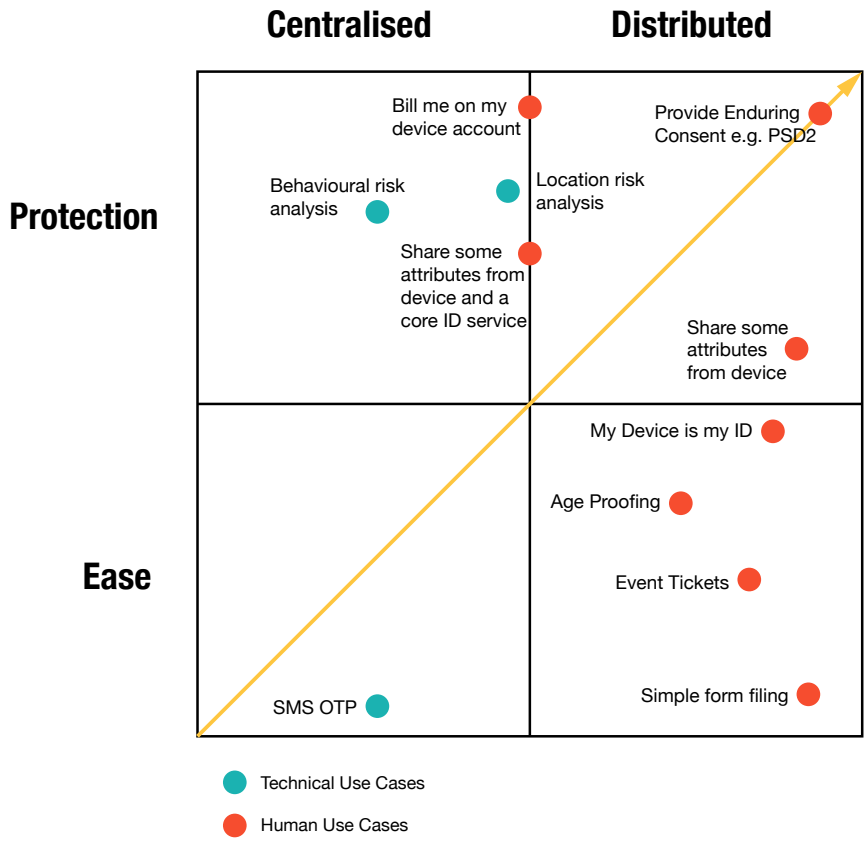
Identity data and PII can comprise a combination of static, dynamic and inferred data, and can potentially be combined with application specific data management requirements. For example, HIPAA compliance is required for health data sharing applications relating to medical 'wearable' devices. It is conceivable that we will soon see dynamic, privacy, and identity-driven routing rules being applied to sensitive health data being streamed from medical wearables.

There is also a security and risk management dimension to this decision: centralised data stores containing PII data on large volumes of people are an attractive target for cyber criminals. As a result, all storage, processing security, consent and self service management platform decisions need to anticipate how and what data is required, and with what frequency, in order to fulfill the desired market strategy.

The following Technology Strategy decision matrix sets out four alternative strategies based on the combination of market strategy (convenience driven or protection driven) and technology strategy (centralised vs decentralised data store)

	CENTRALISED DATA STORE	DISTRIBUTED (ON-DEVICE) DATA STORE
PROTECTION	**TRUSTED AUTHENTICATION VAULT** This technology strategy is relevant to CSPs aiming to combine limited PII with other data/signals held/ captured by telco, such as real time location. The volume of data, processing capacity, frequency of access and frequency of change requires a central data store	**TRUSTED AUTHENTICATION FABRIC** This technology strategy is required for an ecosystem approach. For example, CSPs looking to collaborate as an IDP alongside Government and financial services organisations. 3rd party data management and access, and use cases requiring specific consent, require a distributed approach to data storage.
CONVENIENCE	**MY DIGITAL IDENTITY ON DEMAND** This strategy is viable for CSPs looking to offer a set of user controlled, mass-market, high volume (low risk) IDP services based on a limited set of PII data held by the CSP in their own BSS platforms.	**MY DIGITAL IDENTITY AT MY FINGERTIPS** This strategy is relevant for CSPs looking to offer specific 'Binary' verification services, e.g.: Consent, Proof of age etc. Using a limited set of PII data that does not change means this can be stored in a secure area locally on the users device.

The diagram below illustrates how the use cases considered in the market strategy section above map to this technology strategy decision matrix.



Conclusions

Becoming a trusted identity provider presents an excellent opportunity for CSPs to generate new lines of service and application revenue whilst maintaining strategic relevance in emerging digital ecosystems. Identity management sits at the heart of enabling the dual goals of robust security and ease and convenience in the customer experience across multiple industry sectors, including banking, retail, insurance, public sector, and healthcare. Developing a core competence and brand reputation around the concepts of digital identity and trust will also serve CSPs well in the expanding IoT market, where the concepts of identity, security, and trust broaden from people to the wider world of things and devices.

Fundamentally, however, CSP companies are not going to be the sole custodians of identity. CSP strategies for launching IDP services need to be both open and dynamic in their approach to encompassing external sources of data from 3rd parties within ecosystems. Embracing this requirement, ForgeRock's IDP solutions enable CSPs to grow and develop their service offerings over time. For example, CSPs may launch an initial service based on Mobile Connect to provide mass-market convenience for consumers using distributed data stored locally on their customers' mobile devices. However, once critical mass of users and service providers is achieved, in parallel with building their IDP brand awareness and LOA capabilities, they may then expand their service offerings out across the market strategy map. For example, they may provide a centralised Authentication Vault for some specific target industries and then ultimately provide the Authentication fabric right across target digital ecosystems, as a trusted data aggregation control hub. In this scenario, the value that the CSP brings to the ecosystem operates in many dimensions beyond monetising data. They also provide convenience to consumers, a trusted identity service for service providers, and a neutral Identity management hub for ecosystem collaborators.

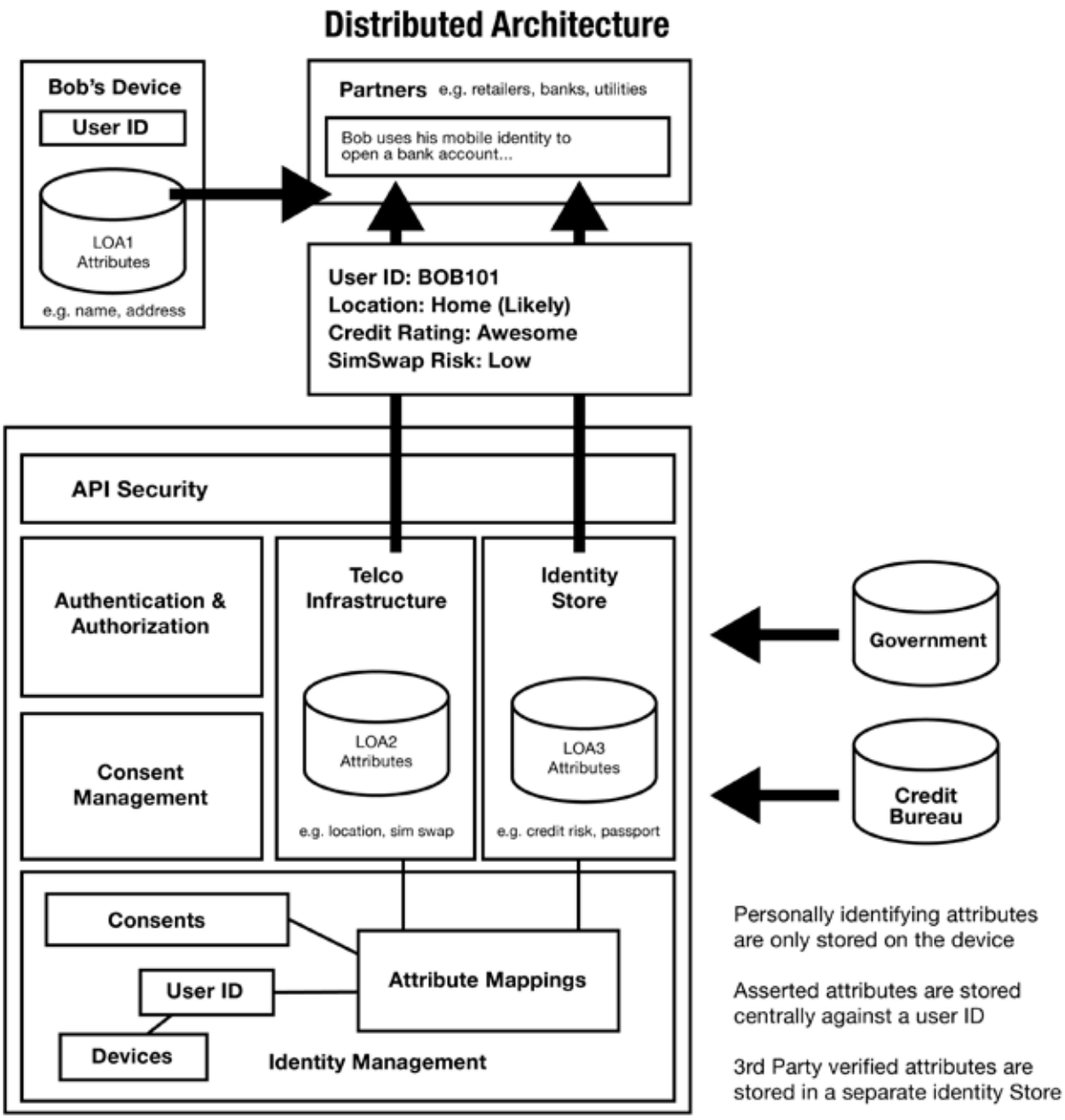
The value inherent in that last point should not be underestimated. In reality, many identity-related data attributes have a 'half life.' For example, people move or change banks. The option to 'verify and forget' is limited and keeping data current is a difficult challenge. CSPs need to consider how their IDP service will be maintained over time, and how this can efficiently and effectively be achieved while keeping with the type of IDP service they offer.

The ability to combine consumer convenience with protection is perhaps the 'perfect' solution when a consumer is obligated to maintain their own digital ID attributes. They are motivated to do so willingly, using well designed self service tools, due to the convenience and security this adds to their lives.

The hybrid architecture for this evolving strategy would look something like the diagram on the following page.

An example hybrid architecture for this evolution strategy is shown below:

Example High level Hybrid Architecture



/ABOUT FORGEROCK

ForgeRock®, the leader in digital identity management, transforms how organizations build trusted relationships with people, services, and things. Monetize customer relationships, address stringent regulations for privacy and consent (GDPR, HIPAA, Open Banking, etc.), and leverage the internet of things with ForgeRock. We serve hundreds of brands, including Morningstar, Vodafone, GEICO, Toyota, and Pearson, as well as governments like Norway and Canada.