MARKET PERSPECTIVE

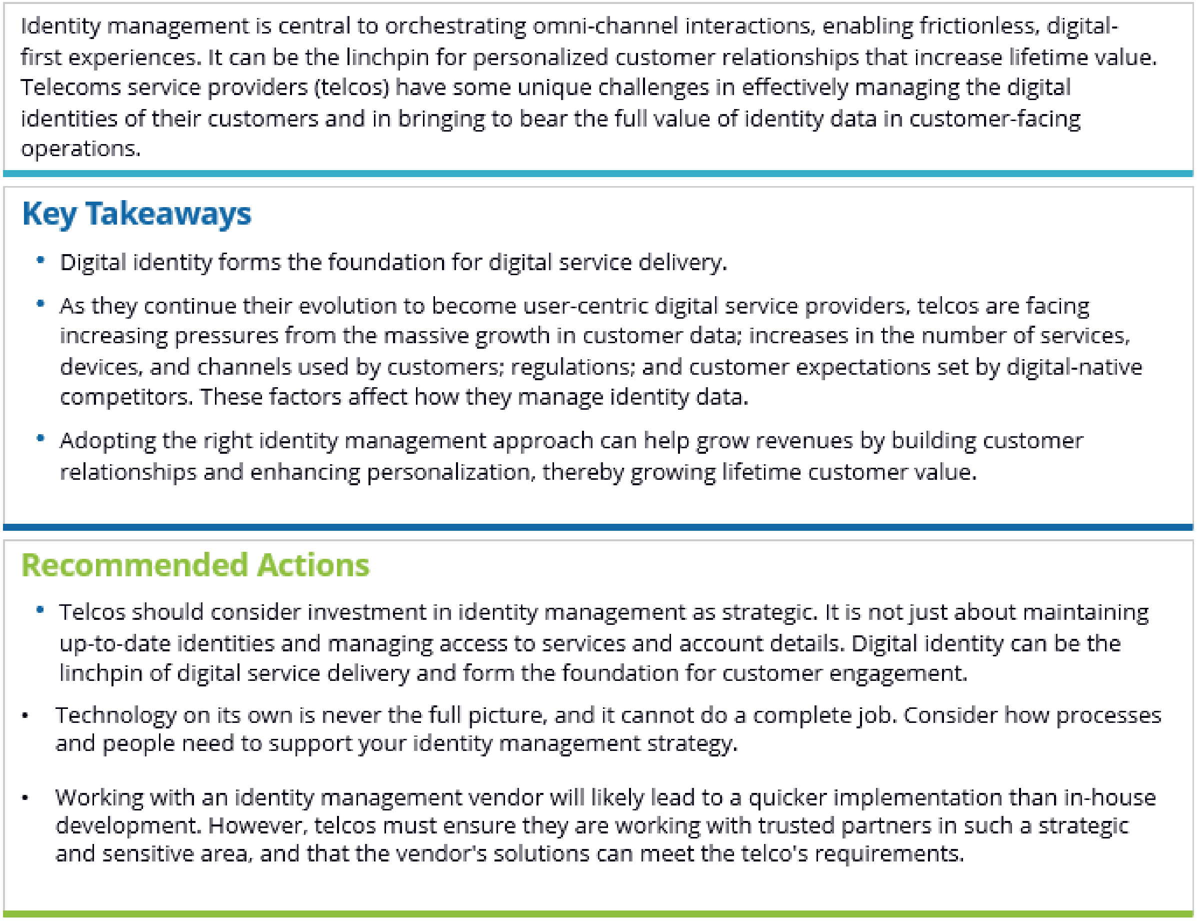
Identity Management: Increasing Telcos' Customer Centricity and Revenues

Rosalind Craven

EXECUTIVE SNAPSHOT

FIGURE 1

Executive Snapshot: Identity Management



Identity management is central to orchestrating omni-channel interactions, enabling frictionless, digital-first experiences. It can be the linchpin for personalized customer relationships that increase lifetime value. Telecoms service providers (telcos) have some unique challenges in effectively managing the digital identities of their customers and in bringing to bear the full value of identity data in customer-facing operations.

Key Takeaways

- Digital identity forms the foundation for digital service delivery.
- As they continue their evolution to become user-centric digital service providers, telcos are facing increasing pressures from the massive growth in customer data; increases in the number of services, devices, and channels used by customers; regulations; and customer expectations set by digital-native competitors. These factors affect how they manage identity data.
- Adopting the right identity management approach can help grow revenues by building customer relationships and enhancing personalization, thereby growing lifetime customer value.

Recommended Actions

- Telcos should consider investment in identity management as strategic. It is not just about maintaining up-to-date identities and managing access to services and account details. Digital identity can be the linchpin of digital service delivery and form the foundation for customer engagement.
- Technology on its own is never the full picture, and it cannot do a complete job. Consider how processes and people need to support your identity management strategy.
- Working with an identity management vendor will likely lead to a quicker implementation than in-house development. However, telcos must ensure they are working with trusted partners in such a strategic and sensitive area, and that the vendor's solutions can meet the telco's requirements.

Source: IDC, 2020

NEW MARKET DEVELOPMENTS AND DYNAMICS

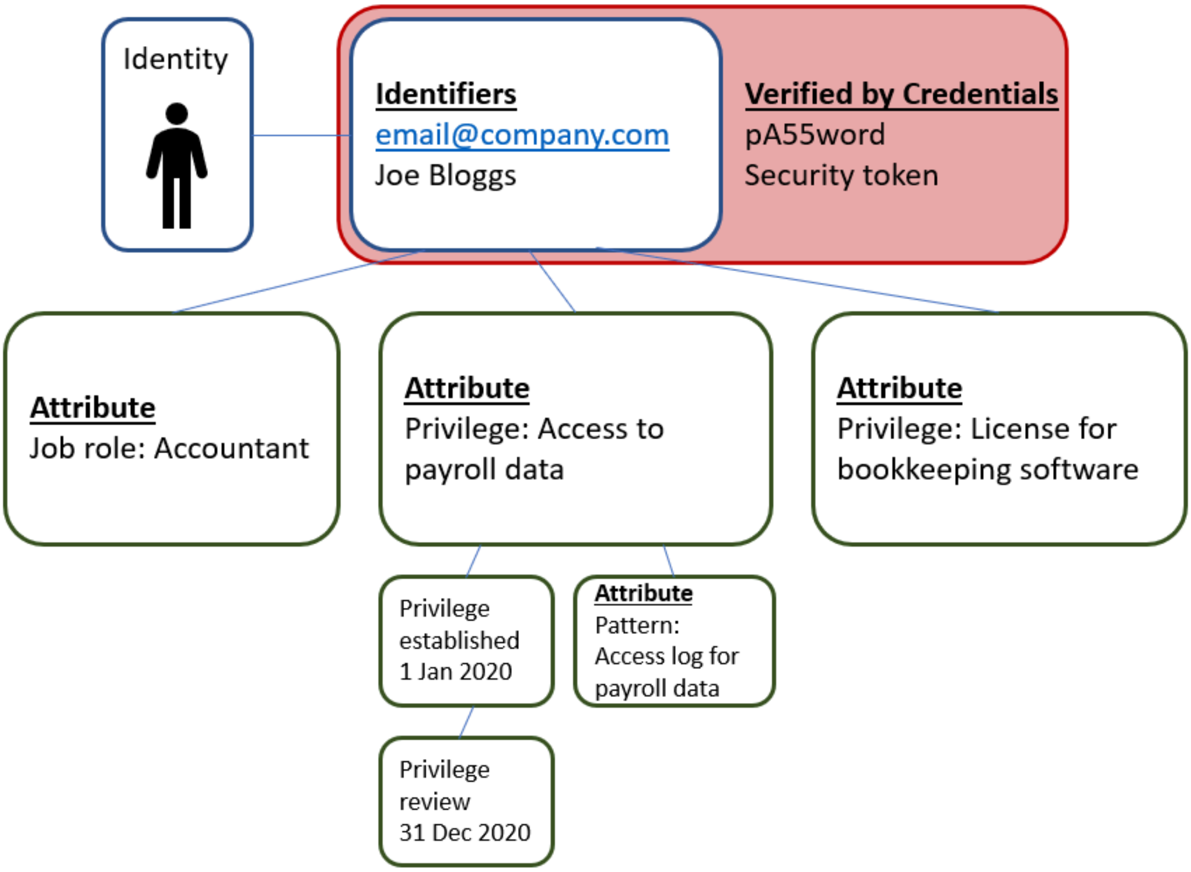
Identity management is central to orchestrating omni-channel interactions, enabling frictionless, digital-first experiences. It can be the linchpin for personalized customer relationships that increase lifetime value. Identity management is thus a strategic imperative for telcos as they transition to become digital service providers (DSPs). This document explores these ideas and the challenges that telcos face in harnessing digital identity to optimize their customer-facing operations. The document will help CDOs, CMOs, and business unit leaders who want to implement identity strategies. This document will focus on the internal role of identity management in telcos' customer facing systems, and it will be followed by an additional report later in the year focusing on services that extend telcos' identity capabilities outside their organizations.

Digital Identity to Telcos: Why is it Important?

Put simply, a digital identity is a database record of an entity that includes information to enable authentication and authorization, and any additional data necessary to deliver a given service. Most people possess multiple digital identities, each with its own identifiers, credentials, and attributes (e.g., an employee's corporate digital identity). Typical identifiers would be name and corporate email address, credentials might include a password or biometric data, and attributes could include the employee's role within the organization, what privileges that role grants the employee in terms of access to company systems and shared resources, patterns of behavior such as time and place of accesses to company systems, etc.

FIGURE 2

Digital Identity: Example

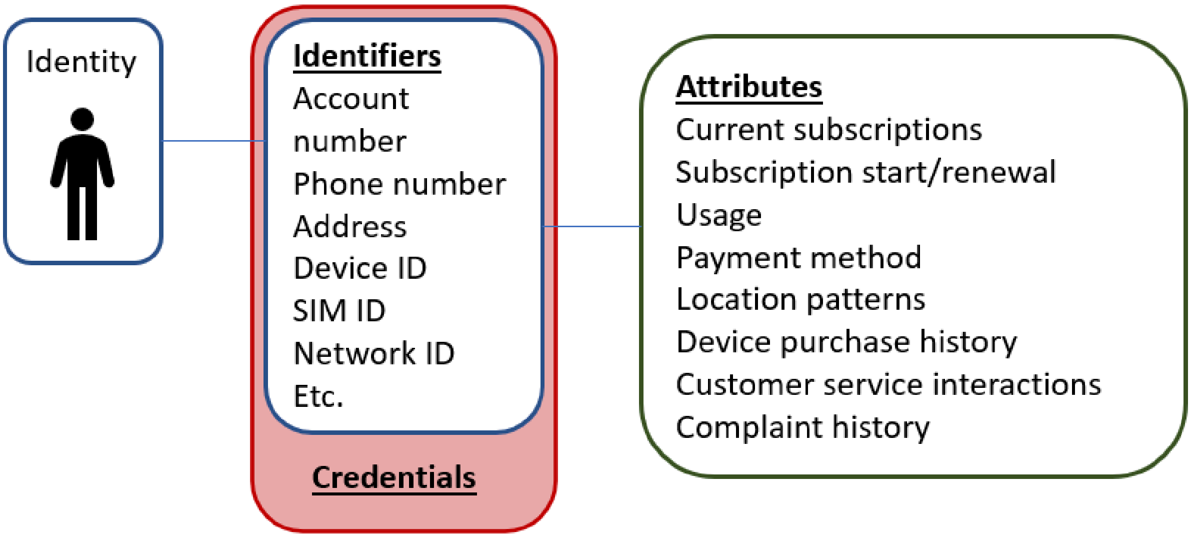

Identity
Identifiers
email@company.com
Joe Bloggs
Verified by Credentials
pA55word
Security token
Attribute
Job role: Accountant
Attribute
Privilege: Access to payroll data
Attribute
Privilege: License for bookkeeping software
Privilege established 1 Jan 2020
Attribute
Pattern: Access log for payroll data
Privilege review 31 Dec 2020

Source: IDC, 2020

In a traditional telecoms context, the entity is usually a customer, though it could also be a device in some circumstances. Identifiers might include a customer or account number, an address, a phone number, a device ID, a SIM ID, or a network ID. Credentials could include passwords, security questions, or digital certificates. Attributes might include subscription details that will specify what services an identity has a right to access, usage and billing information, or history of contact with customer services.

FIGURE 3

Telecoms Digital Identity: Examples



Source: IDC, 2020

Telcos' network and operations consist of multiple functional elements that use identifiers of entities to perform their functions to support and facilitate services and applications. This means different identifiers and attributes are stored and used in different network and support system elements, as they are needed to perform those elements' specific tasks. That could include a business support system (BSS) for mobile services using an account number, SIM identity, subscription plan privileges, and usage data to help generate a bill. It could also be an IPTV supporting BSS approving access to a given premium channel based on account number, device ID, and attributes detailing which channels have been added to the subscription. Or it could be a CRM database granting a customer access using their account number and password to view their account details and change subscription plan. Digital identity is a necessary element in systems designed for delivering and administering services.

Telcos are now transforming into customer-centric digital services providers. As this transformation takes place, it brings with it new pressures and complexities that affect how telcos use digital identity.

- **Increase in services, channels, and devices**. Telcos are delivering multiple services in terms of connectivity, content, and cloud, and the idea of what telecoms services are is shifting and expanding. The number of channels through which customers can access their services has likewise multiplied, as has the number of devices that customers may use. This means one customer may have many additional aliases and identifiers across services and devices that need to be recognized as part of the same identity, and back-end systems need to exchange identity data with multiple new front-end channel systems.

- **Data explosion**. Customer data has multiplied a thousandfold in terms of volume and types/sources of data. The concept of what data is "needed" to deliver a service has expanded significantly, as data from customer interactions and usage helps to personalize services, optimize network performance, and so on. Structured and unstructured data from multiple system feeds that describe usage of services, webpage views, and interactions with chatbots and agents, customer comments, survey responses, etc. need to be correctly linked to an identity, alongside basic customer data such as name, address, demographic data, and billing methods.
- **Regulation effect**. The GDPR demands that personal data be secure and that data processing has explicit customer consent. This includes identity data and any data relating to the identity, which puts demands on how identity data is stored and managed. It also requires mechanisms to communicate with individuals about their identity data, in addition to offering options and controls to individuals regarding how their data is used.
- **Customer expectations**. Customers expect a seamless and secure experience as they access and manage their digital services. They expect uniformity of experience across channels, whether digital, in-person, or through a call center. They want privacy and convenience, and their expectations are set by interactions with digital-native companies that have advanced approaches to managing identity. To achieve these kinds of experiences, each system and access point must be able to access the same complete source of customer data, with a unified identity successfully linked with all the appropriate attributes that are up to date in close to real time.

In the past, the distributed approach in which each system and element holding the identity data that it needed to perform its specific task was sufficient for telcos to effectively run their businesses by providing profitable services to their customers. With the developments outlined previously come new demand for comprehensive identity management strategies. This should ensure that each new channel is plugged into the same identity data, that a large number of identifiers and aliases — and a huge quantity of usage, behavior, and preference data — can be accommodated and their relationship with an identity understood, and that there are mechanisms in place to communicate with customers about their identity data.

Implementing a new digital identity strategy, and turning identity management from a challenge to a strength, presents many great opportunities. Telcos that have undertaken or are undertaking significant efforts to implement new digital identity management strategies cite different business objectives that have a number of common themes.

- **Drive customer data collection and profiling, and thus take personalization to the next level.** Telcos want identity management to help them better understand their customers, improve collection and consolidation of customer data across different interactions with different products and services, and in some cases reduce dependency on external data sources for some of their customer profiling. Improved customer data will then enhance personalization, leading to revenue growth through increased customer lifetime value.
- **Build simplified and frictionless customer journeys**. Telcos want to offer frictionless onboarding for new users and new additional services, and for users to have the same experience across multiple services and access channels by utilizing a common identity platform.
- **Ensure regulatory compliance and customer trust.** Telcos want to build trust with their customers by offering security for their services and data and giving them full and explicit control over how their data is used. This enhanced privacy and consent relationship also supports regulatory compliance. Beyond this, enhancing the quality of their databases by ensuring identities are correct and verified helps with fraud prevention and meeting know-your-customer standards. Telcos want an identity management platform that will help do these things more efficiently.

- **Adopt a person-centric approach across IT systems.** Customer centricity is a core value for most telcos, but focusing on the needs of a customer means focusing on the needs of a person, not an account, and these are not always the same thing. Telco IT systems tend to be built around accounts and devices, and they are not innately set up to be person centric, and telcos want to use identity management to build person-centric capabilities across their systems.
- **Avoid expensive and disruptive BSS transformation.** Telcos need to evolve their systems as they transition into DSPs and as services and business models evolve. However, telcos would prefer to achieve identity management goals without an expensive and disruptive back-end overhaul.

For these business goals, focusing on digital identity is unlikely to be the whole solution. However, problems with identity can be a huge barrier, and the right approach to digital identity management will be a significant tool in meeting these goals.

Digital Identity Management: Challenges and Solutions

Telco systems are designed to do the job they need to do, and only that. This fact — combined with the well-established problem of system fragmentation as a result of historically siloed attitudes and the natural evolution of telco services and systems over time — means that while they are adequate to keep services running, these systems are ill-adapted to cope with the new pressures associated with DSP transformation outlined previously. It leaves telcos with challenges to overcome in their identity management strategies.

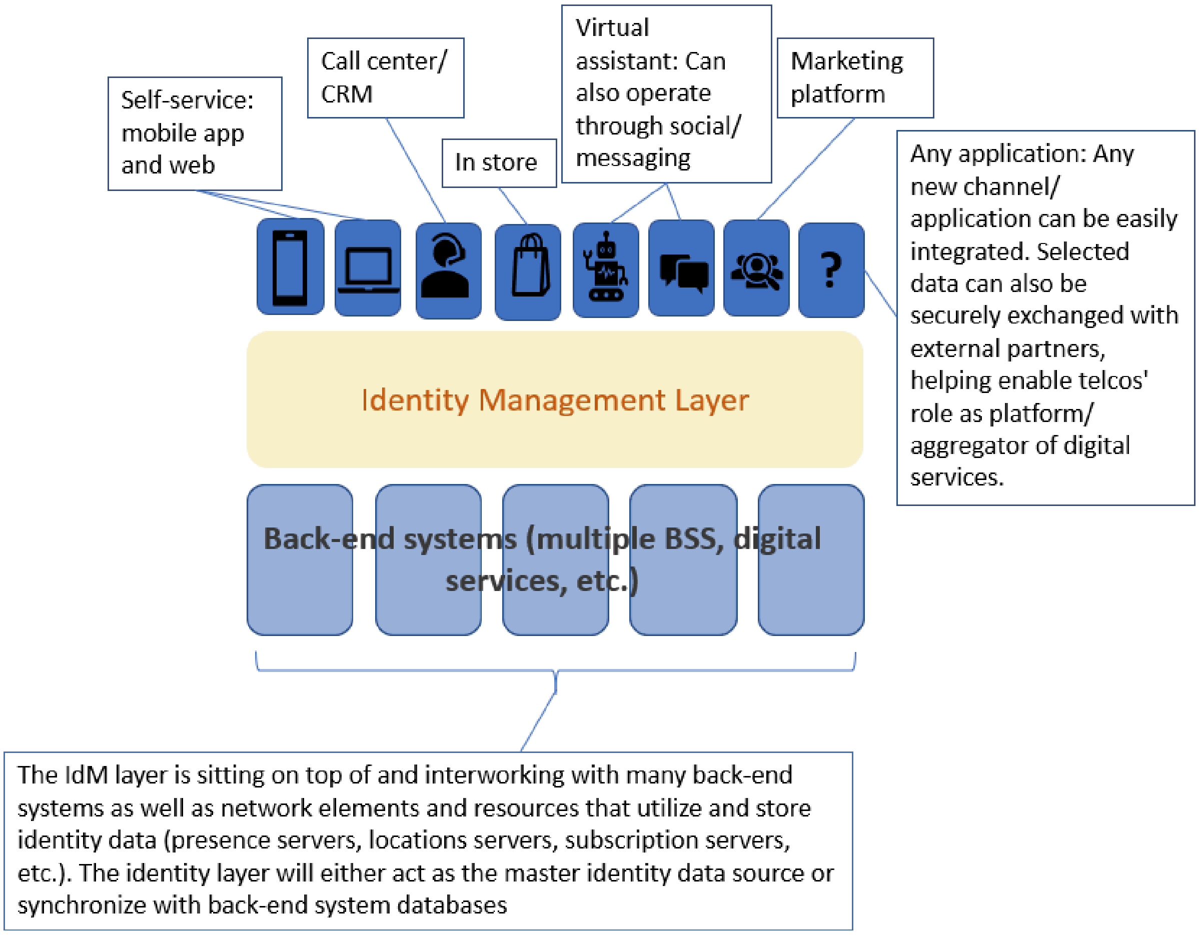
- Multiple versions of customer identity data stored in multiple databases, each in some way incomplete
- Most (if not all) identity databases working on an account centric basis (i.e., they only support one identity per account, which is usually the bill payer) with little flexibility to adapt to different reality of service usage
- Difficulty in determining whether identities across different databases for different services, is in fact the same user or whether the end user of a service is the same as the registered bill payer
- Challenges in incorporating new sources of user data from new digital channels and applications, connecting with appropriate identities, and making such data available to other systems for analysis and action
- Difficulties in scaling databases to accommodate increasing volumes and sources of data as the number of services, devices, applications, and access channels increases
- Some difficulties in achieving smooth single sign-on (SSO) experience for customer across services and channels

Telcos need to establish an identity management approach that will begin to overcome these challenges, address the new challenges brought on by DSP transformation described in the previous section, and help them achieve their identity management business goals. This will mean in some way centralizing identity management, with a common identity layer that can work over the top of back-end systems and support customer-facing applications, providing them with a common, single identity data truth and accepting and incorporating data from them on an ongoing basis. This identity solution will need to fulfill a number of requirements.

- **Successfully interwork with existing BSS and backend systems without disrupting any of their functions or requiring any modification**. One of the desired business outcomes is to avoid expensive BSS overhaul while addressing identity issues. This requires that the centralized identity management platform to act as on overlay to these systems, either replacing system identity databases where interworking is possible or with some form of bidirectional data synchronization where necessary. It will also be necessary to successfully connect all identifiers relating to the same identity.
- **Readiness to interwork with future business enablement solutions.** While telcos want to avoid costly BSS overhauls to solve their identity issues, they must ultimately transform their monetization systems to enable new telco business models based on virtualized networks and end-to-end automation. To be compatible with this evolution, the identity management platform must be cloud native and conform to industry best practices and standards around open APIs, digital architecture, microservices, etc.
- **Accommodate individual user-level identities, and understand relationships between users, devices, services, and account holders**. This is essential for meeting some of the essential business goals of identity initiatives such as achieving advanced personalization, because the target of personalization should be a person, and not just an address or lead account holder who may not be the only person using the services. Being able to manage user life cycles separately from account/purchase life cycles creates new opportunities for relationship building and revenue growth. Moreover, managing consent and privacy on an individual basis not only enhances trust and builds relationships, but could be construed as essential to properly complying with regulations.
- **Support telco agility and faster time to market.** As part of their transformation, telcos are trying to increase their agility. They need to introduce and modify new core and cloud-based services, new channels, and new business models and charging paradigms rapidly to respond to changing market conditions and compete with digital-native companies. It will take agility in other areas such as rules and policy to achieve this, but identity management solutions must support it. This could manifest as an integrated service gateway to facilitate rapid integration, optimizing the central database for real-time queries, or exposing account/user/device/services/relationship data to network or charging functions.
- **Incorporate the latest access management and security protocols**. Under GDPR, all personal information must be secure, and in terms of trust and customer relationships, identity data is seen as particularly sensitive. The security of this data is of the highest priority. Encryption of data at rest, in motion, and in use is essential, as are other features such as tamper-evident logs and limiting data access privileges for admin accounts. Security must be assured not only in the data layer, but also in access and authentication in how customers access their services with features such as multifactor authentication and in how data is shared between applications and with partner organizations.
- **Easily scale to accommodate new data demands**. The expansion in the number of services, devices, channels, and applications as well as the amount of data gathered on customer patterns is already a challenge for current systems. An identity management platform should also be easily scalable to accommodate further expansion of users and devices as well as complexities and volumes of data in the future.

FIGURE 4

Diagram of a Centralized Identity Management Layer


Self-service: mobile app and web
Call center/ CRM
In store
Virtual assistant: Can also operate through social/ messaging
Marketing platform
Any application: Any new channel/ application can be easily integrated. Selected data can also be securely exchanged with external partners, helping enable telcos' role as platform/ aggregator of digital services.
?
Identity Management Layer
Back-end systems (multiple BSS, digital services, etc.)
The IdM layer is sitting on top of and interworking with many back-end systems as well as network elements and resources that utilize and store identity data (presence servers, locations servers, subscription servers, etc.). The identity layer will either act as the master identity data source or synchronize with back-end system databases

Source: IDC, 2020

An identity management solution fulfilling these requirements should fulfill telcos' common business goals for identity management and meet the identity data challenges inherent in DSP transformation, as detailed in the previous section.

These essential requirements can be further enhanced by additional features that will further help telcos achieve their desired business outcomes. As outlined previously, it is essential for an identity management solution to support user-level identities. Some additional features will make it easier to realize some of the benefits of these user-level identities. For example, to ensure they are complying with data protection regulations on consent, telcos will want to have mechanisms to communicate effectively with individual users so as to enable informed decisions and build high-trust customer relationships. They might achieve this through personalized user dashboards, which while they could be built separately could also be incorporated into the core identity management solution. Likewise, to draw the full benefit from their centralized identity data, telcos want to make it easily accessible (as appropriate on a security and privacy basis) to internal users without technical knowledge such as those in marketing and customer care, so optimized internal user interfaces are also a consideration.

Non-technology-focused initiatives will also support the efficacy of technology deployments. The right platform may be able to help connect disparate data to a unified identity, but there are some leaps and connections that are challenging to make as well as gaps in knowledge about users that cannot be filled by correctly assimilating existing data. Telcos that have been most proactive in their identity strategies have not been afraid to ask questions from their customers. This can actually build customer relationships and efficiently fill information gaps.

Additionally, telcos that are very serious about making identity a priority also talk about forming cross-departmental teams to make sure that the ramifications of the user-centric identity approach they are trying to adopt are understood throughout the company and that processes change accordingly. No technology architecture can achieve change on its own.

Implementing a Centralized Identity Management Platform

Telcos have the option of either building their own centralized identity management solutions or contracting vendors. Using a vendor is likely to result in a more rapid deployment, but given the sensitive nature of identity data, the strategic importance of identity, as well as the variety of issues and desired outcomes, some telcos will prefer to develop identity platforms in-house.

- Orange is an example of a telco that has chosen to develop identity platforms in-house. The company has taken on identity and access management as a key strategic priority. It has put in place cross-departmental teams at group level to work on this issue and provide guidance and potentially centralized solutions to local country operations. It is seen not only as an IT issue, but something that requires the rethinking of processes and customer journey structures. Developing in-house may take longer (historically, telcos have tended to remake the wheel when they develop their own systems), but it may encourage a broader view such as the approach demonstrated by Orange, in which processes and culture across the company is considered as part of a drive to increase user-centricity.
- Amdocs' User Lifecycle Management (ULM) platform was designed to be telco specific. This means that it was designed with telcos' identity challenges in mind and built to seamlessly interact with telcos' backend systems. ULM has a full suite of capabilities around digital identity management, making identity a strategic asset for telcos. As the name suggests, it has particular strength in its ability to allow telcos to connect with and manage users as individuals, enabling the management of the user life cycle separately from the account life cycle, so that the telco can establish relationships with each individual user, leading to building lifetime user value.
- Other identity management specialists have also been successful integrating their core offerings into a telco context. Ping Identity's PingDirectory is adopted by many operators across Europe and North America, offering a centralized identity database that can offer bidirectional synchronization with legacy systems where necessary, in addition to offering the flexibility to support new and innovative configurations of accounts, users, and services. Other identity and access management (IAM) vendors active in the telco space include ForgeRock, Okta, and Oracle. These IAM vendors operate cross-industry and have adapted their solutions to a telco context. The only telco-specific identity management vendor to emerge has been UXP Systems, which was bought by Amdocs and assimilated into its portfolio to create the ULM platform.

Identity management appears to be something that most BSS vendors have not invested in specifically, with most apparently viewing it as outside of their scope. Even Amdocs, which now focuses on this area, gained its identity management capabilities through the acquisition of UXP Systems in 2018. UXP Systems was founded in 2011 by industry insiders who saw a need for a telecoms-specific digital identity management approach that offered centralized identity and access management, privacy, security, and consent. These are needed across industries, but with a focus on telecoms-specific concerns such as managing identity with services delivered to households, integrating with back-end systems, and accommodating network data where necessary. The identity and access management space is dominated by horizontal solutions providers, and some have been more successful than others in adapting to a telecoms context.

Future Developments in Telecoms Identity Management

Emerging technologies and evolving telco architectures, relationships and business models will have an impact on identity management in the future

- **Digital twinning**. Digital twinning is a set of emerging technologies that has considerable potential utility for telcos. A digital twin is a digital representation of a real entity, be it a person, organization, process, network, etc. It can be used to simulate and forecast the behavior of the real entity. When it comes to identity and life-cycle management, digital twinning could help further evolve individual-user-based personalization that is enabled by a user-centric identity management model. Twins could be used to simulate on an individual basis how a customer will react to different messaging, very carefully identify the right moment to approach them, or simulate how individual users will be affected by network maintenance or planned changes and trigger actions. Thus, although use-case scenarios are being talked about in terms of individual customer targeting, real-world use of this technique is more likely to be on a cohort basis to reduce the overheads of truly individual modelling. It could also be used to further enhance the security of identity data by enabling external systems that need to interact with the identities use digital twins instead. Without the right data model for user-level identity and associated data, this will not be possible in the first place.
- **Blockchain.** Blockchain is already being used in some identity and access solutions as a means to increase security by eliminating password sharing and giving users control over their digital identity and how it is shared. There is potential for telcos to use blockchain technology in a similar way, and some telcos have expressed interest in using it as a mechanism for giving users more visibility and control over their data and how it is shared, which is particularly relevant as telcos seek a greater role in managing digital identity outside their organizations, as mentioned previously. However, this potential is seen as contingent on the availability of a safe and reliable way to access this information on a blockchain. It is also worth remembering that often, just because blockchain can be used for something, it does not mean it cannot be done just as well — and possibly more efficiently — by other means.
- **Identity as a service**. Current and future identity service opportunities will be examined in depth in the upcoming report mentioned in the introduction. As networks continue to develop (5G, network slicing, edge capabilities, etc.), the way telcos offer services to customer and partners will evolve, with many B2B2X business models emerging and partners accessing aspects of the telco network to build their own services. This emerging paradigm will present telcos with an opportunity to become involved with managing digital identity on a global scale, but that will depend on them having developed a service layer to manage and exchange identities with other parties.

ADVICE FOR TELCOS

- Telcos should consider investment in identity management as strategic. It is not just about maintaining up to date identities and managing access to services and account details – digital identity can be the linchpin of digital service delivery and form the foundation of customer engagement.
- Before implementing a digital identity solution, telcos must consider what their specific needs are and how these may evolve over time. A centralized digital identity management platform can solve many issues at once rather than tackling them individually.
- Telco business models will evolve in the coming years, and so will their supporting technologies. Telcos should be confident that their identity management solutions will be flexible enough to incorporate new technologies as well as support changing business models and business enablement solutions.
- Technology on its own is never the full picture, and it cannot do a complete job. Consider how processes and people need to support your identity management strategy.
- Working with an identity management vendor will likely lead to a quicker implementation than in-house development. However, telcos must ensure they are working with trusted partners in such a strategic and sensitive area and that vendor solutions can actually meet telcos' requirements.

LEARN MORE

Related Research

- *IDC FutureScape: Worldwide Future of Connectedness 2021 Predictions* (IDC #US46921520, October 2020)
- *Consumer Strategies of European Telcos* (IDC #EUR146638120, July 2020)
- *Top CX trends and Challenges for Telcos in 2020* (IDC #EUR146363320, June 2020)
- *European Telecoms in 2020: An Industry Outlook* (IDC #EUR146043220, February 2020)

Synopsis

This IDC Market Perspective explores identity management in telcos and the challenges telcos face in harnessing digital identity to optimize their customer-facing operations. The document explores the business goals telcos can achieve through identity management strategies. It will focus on the internal role of identity management in telcos' customer-facing systems, which will be followed by an additional report later in the year focusing on services that extend telcos' identity capabilities outside their organizations.

"Identity management is central to orchestrating omni-channel interactions, enabling frictionless, digital-first experiences. It can be the linchpin for personalized customer relationships that increase lifetime value. Identity management is thus a strategic imperative for telcos as they transform into digital service providers," said Rosalind Craven, research manager, EMEA Mobility.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC U.K.

IDC UK
5th Floor, Ealing Cross,
85 Uxbridge Road
London
W5 5TH, United Kingdom
44.208.987.7100
Twitter: @IDC
idc-community.com
www.idc.com