FORGEROCK /White Paper

/The 5G Trust Equation:

Network + Identity = Opportunity

WHITE PAPER

The 5G Trust Equation: Network + Identity = Opportunity

Executive Summary

'Leverage the core' is a term often used by communications service providers (CSPs) to articulate their belief that with each new wave of technological advancement in the communications industry there are new business opportunities and associated revenue streams to be derived from the role they play in modernising industrial sectors.

With this in mind, 15-plus years ago CSPs began a journey to explore the power of platforms and APIs in their businesses. Now, with the imminent launch of 5G networking technology to enable the 'Internet of Everything' (IoE), we are on the cusp of another unprecedented explosion of technological change. Connected devices, new innovative applications and services, and disruptive collaborative business models are transforming every industry.

CSPs once again have the potential to leverage what they have learned along the way to re-establish themselves as providers of unique incremental business value beyond the basic connectivity their networks provide. No market or sector is immune to this technology-driven paradigm shift, and the opportunity is profound. Put simply, though, in an industry landscape that has become dominated by new, over-the-top (OTT) players, the key question for CSPs is 'How do we monetise the Internet of Everything?'

One answer to this question lies in understanding the challenges that all businesses face when contemplating how to reap the benefits of this brave new technology world. A day does not go past without horror stories, opinion surveys and cautionary tales loudly proclaiming how in the opportunity gold rush we have forgotten some of the basic rules of doing business. With each DDoS attack, identity theft and data scam, people and businesses alike are becoming increasingly aware of and concerned by the need to ensure that our technology is secure, so that our privacy is respected and our identity protected.

This fundamental need for secure, industrial-scale identity protection across ecosystems of collaborating business entities is fundamental to ensuring Trust in the IoE system, and it represents an opportunity of which CSPs are uniquely positioned to take advantage.

It is against this backdrop that we describe in this white paper how CSPs can incorporate the ForgeRock Identity Platform into their 5G network strategy to deliver telecoms-grade identity and security services into IoE ecosystems.

Equipped with these critical business enablers as a value-added layer incorporated within the 5G network, CSPs will be in a position to establish themselves as the 'Trust Core' of emerging connected ecosystems in the Internet of Everything.

Introduction

With 5G on the horizon, the communications industry and its wider ecosystem will have access to technologies, standards, platforms and business models that will underpin significant portions of consumer and enterprise platforms. Those platforms need to be architected and designed with identity, trust and security in mind, as they will power an ever more interconnected global ecosystem that our daily lives and economies depend on.

Once in place, 5G will power mission-critical as well as leisure-orientated applications. With advances in

networking, computer and software technologies, we are likely to see new inventions and innovations becoming part of our daily lives at a rapid pace. 5G will enable and power digitalisation of businesses that previously have been constrained by technology platforms and lack of global ecosystems, or that haven't had the economies of scale required for mass deployment.

CSPs are developing strategies for how to best capitalise on the investment they are going to make in 5G networks and technologies. Most CSPs are considering how to increase their 'share of wallet' with services that extend and add value to their network assets, systems, data and customer segments. In most cases they want to avoid becoming a mere bit pipe that simply connects network endpoints to an increasingly extensive ecosystem of OTT service providers. 'Leverage the core' is a term sometimes used by CSPs to indicate that new business opportunities and associated revenue streams can be derived from the role a CSP plays in a modern, connected ecosystem. Put another way, the key question for CSPs is 'How do we monetise the Internet of Everything?'

Being the operator of networks and associated systems places the CSP at the core of today's connected lifestyles and businesses. Networks are, as we know, the core enabler for a huge and increasing segment of today's economy. Financial services, consumer leisure services, industry automation, public safety and health care are all examples of major industry sectors that are critically dependent on secure, trusted and reliable networks.

Beyond the network

But it's not just about networks any longer. Increasingly, it is about the trusted, secure and reliable use of those networks, combined with the systems and data to power platforms that form the basis for our increasingly smart and inter-connected consumer and enterprise ecosystems. Fifteen-plus years ago CSPs started (with varying level of success) to explore the power of platforms and APIs in their businesses. There was often a tight integration between the CSPs and their ecosystem partners.

The CSPs have learnt much along the way and now have the potential to both transform and disrupt the landscape that has recently become lost to the OTT players. They have made strategic investments in software companies and extended their portfolios into new types of services, such as managed services for healthcare, smart home/vehicle and industrial IoT, and multi-cloud services to their enterprise clients.

In summary, the CSPs, with their technology partners, are increasingly establishing themselves at a place in our connected ecosystems where identity, trust and security are becoming critical business enablers. This is a trend where ForgeRock can add value not only to CSPs but also to many of their key partners,

MEF MOBILE ECOSYSTEM FORUM

The Mobile Ecosystem Forum 2017 Global Consumer Trust Study

The data and findings cited in this paper are drawn from the Global Consumer Trust Study 2017, commissioned by Mobile Ecosystem Forum. MEF is a global trade body that acts as an impartial and authoritative champion for addressing issues affecting the broadening mobile ecosystem. Established in 2000 and headquartered in the UK, MEF has Regional Chapters across Africa, Asia, Europe and Latin America.

The field study was carried out by On Device Research in Q2 2017 to understand the impact, challenges and opportunities of building trust in personal data. It questioned more than 6,500 smartphone users in 10 countries: Belgium, China, France, Germany, Poland, Romania, South Africa, Spain, UK and USA.

such as device manufacturers, network equipment manufacturers and providers of software applications, platforms and services.

With ForgeRock, identity relationship management (IRM) extends from online services and Operations Support System/Business Support System (OSS/BSS) integration to devices, whether small or large, intelligent or 'dumb'; to network elements such as subscriber management systems; to policy and charging rules function (PCRF); and to the next generation of virtual network functions (VNF) being developed using microservices. The ForgeRock Edge Security and Identity Microservices product modules are our most recent innovations designed to enable CSPs to support deep integration of security and IAM functions into core 5G application enablers.

In this white paper we will further explore and show how the ForgeRock Identity Platform, strategy and industry engagements will enable CSPs and other 5G ecosystem participants to launch trusted, secure and identity-aware platforms for today's and tomorrow's globally connected society.

> *When asked why they don't use more apps and services, 40% of respondents named one or more trust issues as the most important barrier.*
>
> MEF MOBILE ECOSYSTEM FORUM

IoT ecosystems and identity relationships

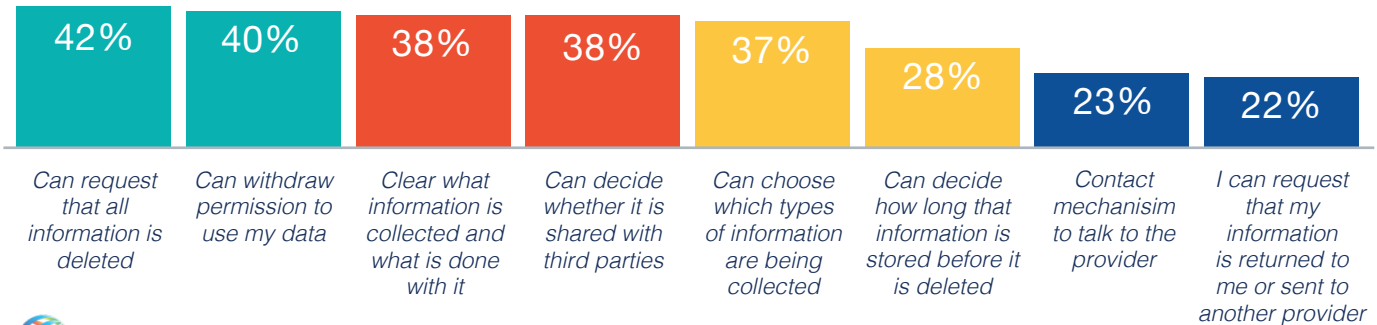
A key enabler and catalyst for creating global, application-driven ecosystems is the role of secure and trusted assertion of the identities of users, devices, networks, platforms and software that the stakeholders will interact with. The velocity of change and the rapid introduction, driven by innovation, of new digital services will drive the need for making the whole ecosystem identity-aware, trusted and secure. Understanding the relationships between identities becomes paramount.

At the same time, the velocity of change must not put the ecosystem stakeholders at risk when it comes to providing, storing and processing sensitive information. For example, with initiatives such as GDPR and PSD there are severe financial penalties for mismanaging information and data that a stakeholder has been entrusted with.

Consumers will expect that their chosen identity providers can be trusted to use data only for the purpose they were provided for. Stakeholders that are collecting, storing and processing such data need to ensure that their platforms and processes are sufficiently robust and effective that data aren't turning into 'toxic waste', with associated liabilities and penalties.

5G standards and platforms will change the nature of connected applications and ecosystems. The industry has evolved from the days of analogue

Which of the following would help you have more trust in how an app or service uses your data?



MEF MOBILE ECOSYSTEM FORUM

and early digital mobile phone systems that were targeting voice and message communications. We have seen data rates increasing, latency going down, and operations and management increasingly being automated.

With 5G we can expect:

- Devices capable of connecting at 1 to 10 Gbps or more
- Latency in the 1ms range
- 90-percent reduction on network energy usage
- 1000x increase in bandwidth per unit area
- 10x to 100x more connected devices
  (Source: GSMA)

Security and subscriber privacy protections have improved (e.g., pseudo-IMSI management) and the role of trust and identity are top of mind in the industry. That is reflected in initiatives such as 5G-Ensure, which will provide input to the 3GPP and ETSI standardisation processes. ITU has also finalised their vision for a mobile broadband-connected society.

Industry groups such as TM Forum and Mobile Ecosystem Forum (MEF) are also active in equipping the industry ecosystem for the arrival of 5G.

The 5G ecosystem participants will, amongst others, be:

- Communication Service Providers (CSPs)
- Consumers
- Enterprises
- Device manufacturers
- Governments
- OTT providers
- Application providers
- System integrators (SIs)
- Network equipment providers (NEPs)
- Standards bodies and regulators

Identity at the ecosystem core

Powering the 5G ecosystem will be an array of platforms. Indeed, 5G will further manifest and push the platform-based business and economy forward. However, without secure and trusted APIs that also perform to meet real-time or near-real-time performance requirements, the platform-based philosophy will abruptly stall.

As CSPs are seeking to unlock new revenue opportunities by leveraging their core assets such as subscribers, networks, systems, authenticated billing relationships and trusted branding, we can expect to see an emergence of platforms for a variety of new applications. Mission-critical consumer, community and industrial applications and immersive leisure applications will be built on secure, trusted and identity-aware networks and platforms.

The CSPs are ideally positioned in the ecosystem and value chain to capitalise on their investments and at the same time power an open and global ecosystem. With the explosion in the number of connected devices and, at times, associated subscriptions, a CSP is ideally positioned to act as a secure and trusted identity provider spanning subscribers and devices. CSPs are also ideally suited to provide and leverage IRM services, as they will be able to provide insights into how users, devices and services are linked and used.

Applications that we can expect will thrive when powered by 5G are:

- Smart cities (smart societies)
- Connected and autonomous vehicles
- Immersive media applications
- Health care applications
- Public safety applications
- Industrial applications
- Agricultural applications

Fundamental and critical to the success of 5G applications is to ensure that trusted, secure and identity-aware interactions are at the core of each stakeholder's platforms and systems. Consumers and businesses alike will expect that security, privacy and consent are intrinsic to the applications, devices, things, networks and services they interact with. In the same way that security cannot be an afterthought, privacy and consent capabilities

must be seen as core business-enabling functions and must be considered from day one. Using the ForgeRock Identity Platform and the services it provides will enable identity providers, service providers and application developers to base the privacy and consent features on a standards-based, open and scalable platform.

The emergence of 5G and related technologies and standards will put a strong emphasis on:

- Identity for devices, subscribers, software, network elements and ecosystem participants
- Trust to make mobile subscriber tracking harder outside of the network by leveraging pseudonymous customer reference (PCR) between a telco IDP and relying parties; for example, using GSMA Mobile Connect or pseudo-IMSIs
- Security; for example, asserting identity of a device, its owner, its user and the data it emits

Identity:

- As relevant, the identity (or pseudonym) of the parties in an interaction can be proven.
- As relevant, identity information will form a core context of each and every interaction.
- Double- and triple-blind interactions should be supported.

Trust:

- Data are used for exactly the purpose and intent they were made available for.
- Data can be managed by users and authorised representatives such as enterprise use cases.
- Data can be proven to originate where they claim to come from.

Security:

- Each ecosystem can assume that data haven't been compromised.
- Interactions can be guaranteed to be between authenticated and authorised parties.

> *Privacy (16%) remains the most influential trust-related concern, closely followed by security (15%).*
>
> MEF MOBILE ECOSYSTEM FORUM

A platform-based approach

ForgeRock customer identity and access management (CIAM), identity relationship management (IRM), privacy and consent, edge security and microservices features are key enablers for 5G platforms and 5G-based applications (for example, in healthcare, connected vehicles and public safety). A platform-based business model for an extensive ecosystem is seen as a core 5G characteristic. The platforms will support applications that can leverage 5G platform services, such as 5G network slices, that are tailored to provide characteristics like low latency, high bandwidth and delay tolerance.

The ForgeRock platform can be leveraged across devices, networks and services in a 5G model. Our focus on IoT and microservices positions us well for edge and device use cases as well as for building core network element functions such as OEM with NEPs. This, in combination with our established strength for Identity Provider/Service Provider (IDP/SP) at scale, opens up opportunities for broad and deep conversations with a CSP's product, marketing and technology leads as well as with IT.

5G network-level identity creates new business opportunities

The following key characteristics and features of a 5G ecosystem create new application- and platform-driven opportunities and challenges:

- Lower latency, enabling real-time-sensitive applications such as autonomous/connected vehicles, smart cities and industrial IoT
- Higher bandwidth in the access network and in terminals like mobile devices, enabling immersive media applications and health applications (for example, for first responders) and security and public safety applications

- Network slicing, enabling application-aware networks in IoT applications, for example
- IoT applications for health and security, managing large amounts of sensitive data and requiring user controls for privacy and consent
- Mission-critical applications for connected and autonomous vehicles, smart infrastructure and public safety, requiring trusted, secure and real-time interactions and policy decisions

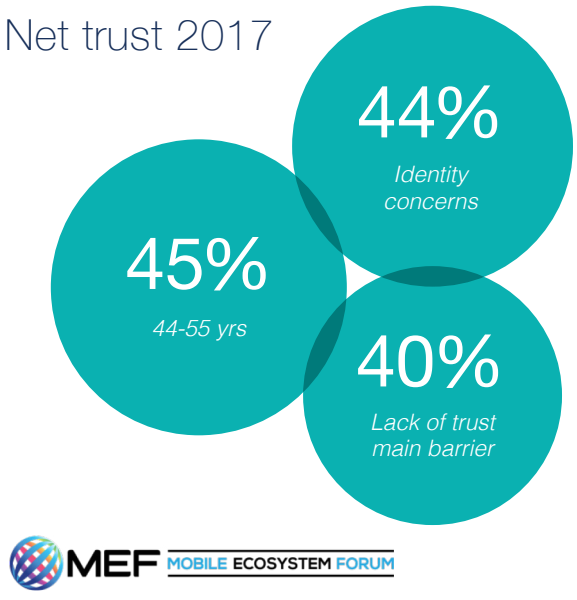
Underpinning the new opportunities are identity, trust and security. Those aspects are becoming increasingly important as 5G applications are making their way into consumer and business ecosystems.

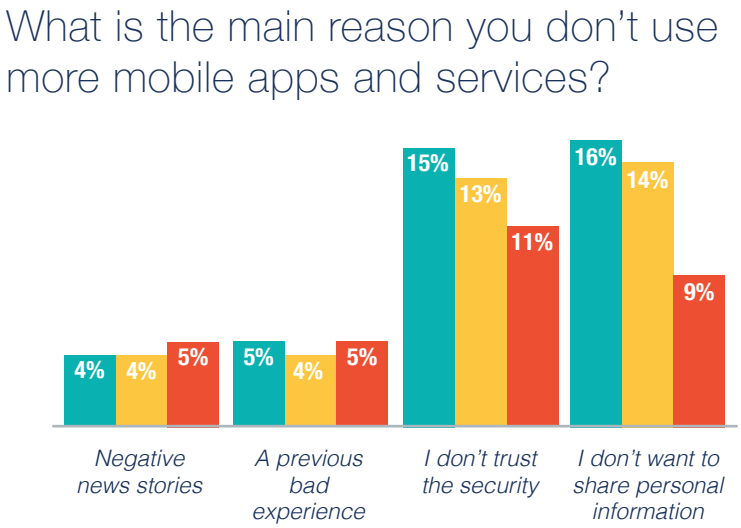
> *'5G-ENSURE will define and deliver a 5G Security Architecture, shared and agreed with various 5G stakeholders.* ***Identity management and privacy-preserving mechanisms are treated as key enablers and anchored against a common security architecture to increase assurance and confidence in 5G networks. Trust, therefore, will influence development, adoption and business potential.***
>
> *'The outcome is a trustworthy 5G system offering reliable security services to customers with a "zero-perceived" downtime for service provision.'*
>
> - ***From 5G-ENSURE Pillars***

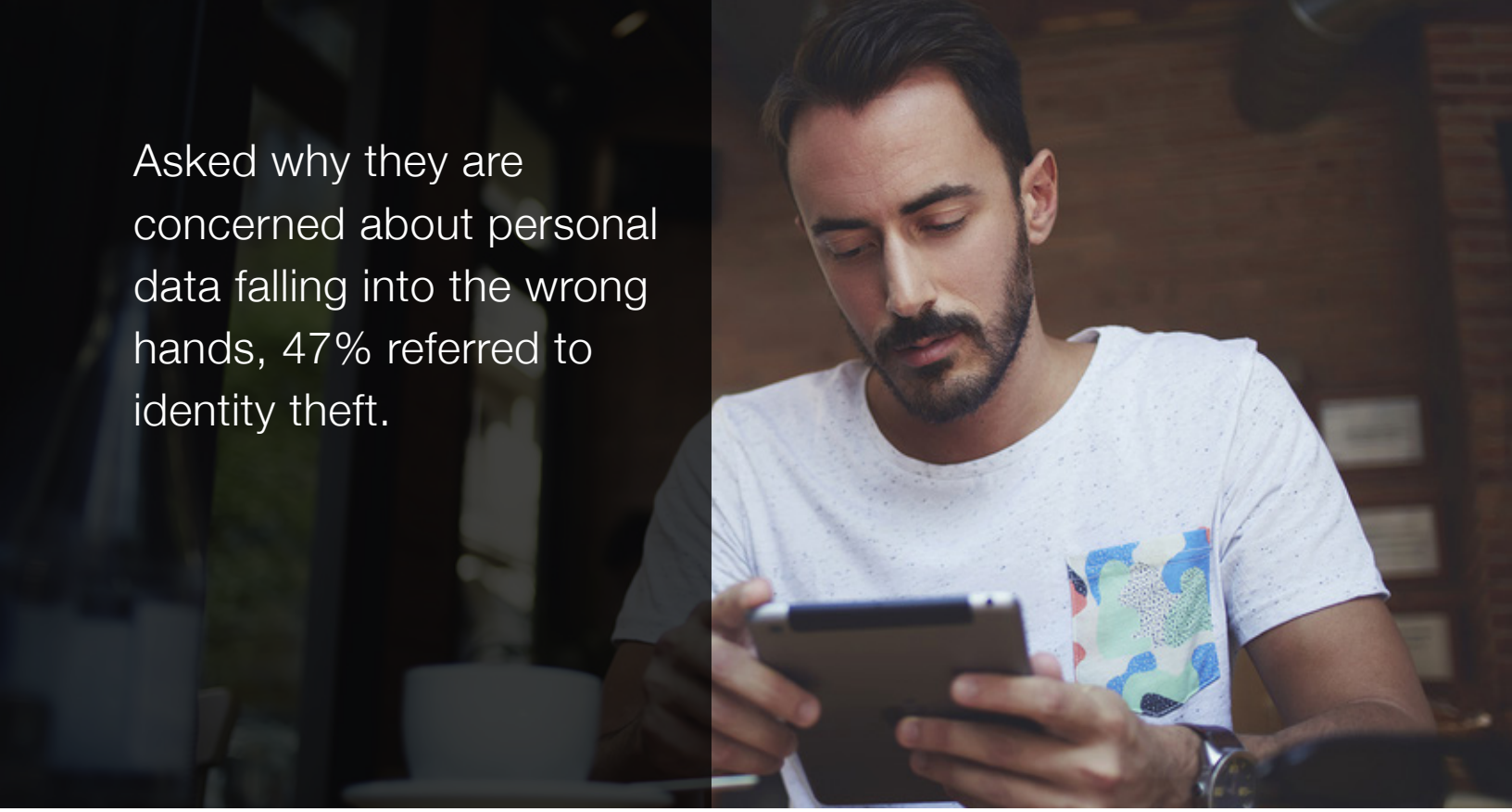
The industry is researching and trialing 5G technology, establishing standards and considering business models and ecosystems. We are at a point in time where CSPs can lay a foundation for business models where their core assets and new platforms will allow them to play a significant and critical role in future value chains.

CSPs maintain well-known and trusted brands in the market. By embracing identity-driven applications and services, they can become the trusted identity provider for their customers. This is true for consumer as well as enterprise markets, spanning humans, enterprises, devices and things. In the same way, 5G platforms will provide end-to-end enablers for CIAM, ranging from on-device trusted execution environments (TEEs), through subscriber identity modules, to standards-based integration with IAM services and platforms.

Increasingly, 5G platforms will power mission-critical applications that require secure and trusted interactions. Assertions around identities, attributes, data and access will often need to be done in real time. This opens up a unique opportunity for CSPs to bring CIAM platforms close to the networks, users and devices that are using a 5G application. Leveraging the concept of a carrier-grade cloud, CSPs can deploy CIAM services in such a way that latency for policy decisions (authorisations) is reduced and network traffic patterns can be used to elastically scale the CIAM platform. A carrier-grade cloud can be described as a deployment environment with characteristics that







are geared towards communications and real-time-sensitive applications.

Some examples of roles a CSP can play in 5G ecosystems are outlined below:

- Trusted identity provider
- IRM aggregator, attribute broker, digital claims verifier and gateway between technology ecosystems (for example, through token translations) and trust boundaries such as maintaining anonymity
- IoT platform provider or IoT virtual platform provider (for example, a mobile virtual network enabler, or MVNE), enabling rapid onboarding for innovative device- and things-providers and an already connected customer base that trusts the CSP's IDP
- Application platform provider for applications that lend themselves towards leveraging a CSP's core capabilities, including networks, systems, subscribers and devices

> *86% took action as a result of trust concerns, including warning friends and family and using a competitive service.*

MEF MOBILE ECOSYSTEM FORUM

Case study: The emerging automotive ecosystem

ForgeRock is an active member of several industry organisations involved in the design and specification of emerging 5G ecosystems and applications, including:

- Automotive Grade Linux
- TM Forum
- Mobile Ecosystem Forum
- Kantara initiative for user-managed access (UMA)

> *'ForgeRock is a member of the Automotive Grade Linux group (AGL), an organization founded to produce a cost-effective, secure, open source baseline Linux platform for modern infotainment and other connected code-driven vehicle systems. Our vision is to authenticate users with the cloud-based ForgeRock identity service so vehicle owners, drivers, maintainers, and renters can have a highly personalized experience.'*

The EU's Fifth Generation Communication Automotive Research and Tnnovation (5GCAR) project is also exploring how 5G will enable an overall architecture for V2X (vehicle-to-anything), where security and privacy are core and critical aspects. One of the project's objectives is to:

> *'Develop an overall 5G system architecture providing optimized, end-to-end V2X network connectivity for highly reliable and low-latency V2X services, which supports security and privacy, manages quality-of-service and provides traffic flow management in a multi-RAT and multi-link V2X communication system.'*

It's a whole new IoT world

As we can see, we are already at a juncture where previously separate ecosystems are converging and becoming critically dependent on identity, trust and security. The aformentioned organisations, in conjunction with standardisation activities that are ongoing in ITU, 3PP, ETSI, 5G-PPP, IETF and GSMA, will set the standards framework for how platforms, devices and applications are going to be built in a 5G environment. From the identity, trust and security point of view, ForgeRock is supporting and leveraging standards like OIDC, OAuth2 and UMA that will allow participants in a global 5G ecosystem to engage in secure and trusted interactions.

> *Almost half (47%) would recommend a trustworthy app to friends and family.*
>
> MEF MOBILE ECOSYSTEM FORUM

Maintaining minimum viable identity profiles

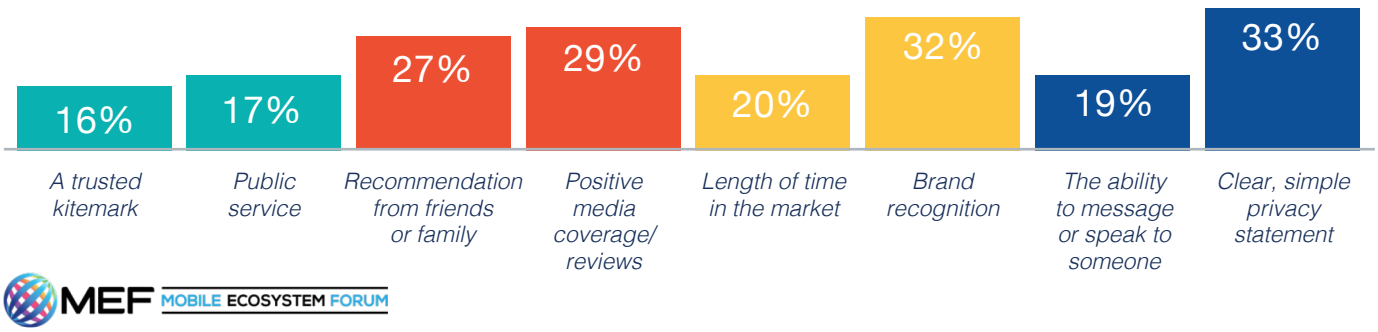
ForgeRock is a visionary and leader in applying IAM to people, devices, software and things such that CIAM becomes a core and critical enabler for connected, innovative and dynamic ecosystems. Customers will expect that starting to use a new device or service, be it a health sensor, a sports car or a home security service, will take advantage of data the ecosystem participants already should know and have been given permission to use. Customers will also expect that the concept of a minimum viable user profile will apply.

A minimum viable user profile will provide just enough data to start consuming a service or using a device. Only essential data that are absolutely required for delivery of a service or the use of a device should be required. This concept will reduce the risk of unnecessary proliferation of personally identifiable information (PII) and provide means for more efficient management of PII and other sensitive data. At ForgeRock we believe that it should be possible for privacy and consent management to be under the control of the user or properly authorised delegates and representatives.

In 5G ecosystems, we can expect more dynamic interactions facilitated by fast and secure networks, for example, between a device such as a car and sensors in a smart city, or between cars themselves. A trusted identity provider such as the CSP will act as the gate to ensure that only relevant data are shared.

For example, a smart city system may only need to know that a driver of a vehicle is appropriately authorised to request, using vehicle-to-smart-city sensors, a green wave

What is it about an app or service that makes it trustworthy?



MEF MOBILE ECOSYSTEM FORUM

of traffic lights, because the driver is acting in the role of a first responder. Smart-city infrastructure and vehicles are prime candidates for leveraging 5G technologies and applications. In the matter of command and control of critical infrastructure, it goes without saying that the interactions must be secure, trusted and identity-aware.

> *When asked what makes an app or service trustworthy, 33% said a 'clear, simple privacy statement'.*
>
> MEF MOBILE ECOSYSTEM FORUM

Establishing trust: In the cloud, at the edge, through gateways

The viability of 5G applications will depend on the trust and security of sensors, sensor data, users, devices, networks and services. Devices, sensors and services increasingly offload tasks from the human user in order to assist, optimise and increase productivity. Therefore, it is critical that hardware and associated services be secure and that data and operations be trusted. Decisions are increasingly going to be made on trusting digital claims asserting certain attributes of a user, device or sensor data.

Enabling scenarios like the ones given above is an example of how IRM can be applied in combination with Identity Edge Security, Identity Microservices and Customer IAM. IRM will allow the system to understand how the vehicle, the driver, the traffic management system, the first responder ERP system and other participants relate to one another and which policies apply based on the active relationships. Identity Edge Security features such as the ForgeRock Identity Edge Controller (IEC) and the ForgeRock Identity Message Broker (IMB) will be actively used to ensure that relevant entitlements are provisioned to the vehicle and that messages emitted can be proven to be authentic and valid.

The vehicle will need to communicate with the traffic management system and with other vehicles as relevant, even if full network coverage is not available. In 5G it can be anticipated that network base stations will be able to provide assisted communications even in the event of a core network failure. Another mechanism under consideration is to establish mesh networks where each node in the mesh will try to pass a message on until it reaches its ultimte destination. Research into disruption- and delay-tolerant networking (DTN) is also important to communications resilience.

ForgeRock Identity Microservices will, amongst other things, allow just enough contextual identity information to be associated with each request to ensure that the request is being serviced in a secure, trusted and auditable fashion. 5G platforms and applications will be more real-time-sensitive and increasingly be deployed on platform as a service (PaaS) using microservices architectures. Having native identity microservices deployed to the PaaS platform will enable the creation of truly identity-aware applications where relevant, contextual identity information is included as tokens in each and every service interaction. This will allow not only for greater end-to-end security and auditability but also for a higher degree of autonomous computations.

CIAM is the cornerstone of a CSP's trusted IDP capabilities in 5G. The ForgeRock platform can be deployed in the carrier-grade cloud, which is typically close to the networks and application platforms.

Downstream network integration can leverage ForgeRock Identity Gateway and ForgeRock Edge Security features. Upstream access to the trusted IDP services and the CSP exposure to the 5G ecosystem can leverage the ForgeRock Identity Gateway and the standards-based services the ForgeRock platform natively provides. Horizontal integration amongst the ForgeRock platform services and adjunct CSP systems is facilitated by standard protocols, APIs and frameworks.

It should also be noted that the ForgeRock platform and technologies are highly relevant to 5G network equipment providers, software application providers and systems integrators that work in the core network domain. It is anticipated that network elements and network software increasingly are going to leverage standards such as OIDC and OAuth2 for identity and security enablers.

5G architectures make extensive use of network slicing as a means to provide appropriate and tailored capabilities for certain applications. For example, a network slice can be dedicated to connected vehicles and configured to secure and facilitate interactions for V2V (vehicle-to-vehicle), V2P (vehicle-to-pedestrian), V2I (vehicle-to-infrastructure) and V2C (vehicle-to-cloud) scenarios.

It is worth pointing out that a network endpoint, such as a vehicle, can be attached to several different network slices at any point in time. For example, vehicle telemetry and traffic management system interactions take place in a connected-vehicle slice, whilst the onboard vehicle infotainment systems are connected in a streaming-media slice. ForgeRock is well suited, thanks to IRM, to leverage how an endpoint and its associated users are attached to various network slices. From an CSP-trusted IDP point of view, IRM comes together in the ForgeRock CIAM platform.

Real-time authentication on a massive scale

No doubt 5G will power mission-critical consumer and enterprise applications that will be real-time-sensitive. Authentication, authorisation and provisioning services will need to be massively scalable to cope with user, device and infrastructure demands. The CSP's CIAM platform should be deployed in a carrier-grade cloud environment that is aware of the networks and applications it serves.

Various 5G network slices will have varying requirements on the CIAM platform.

> *75% say they read a privacy policy or terms and conditions before signing up to a mobile app or service.*
>
> MEF MOBILE ECOSYSTEM FORUM

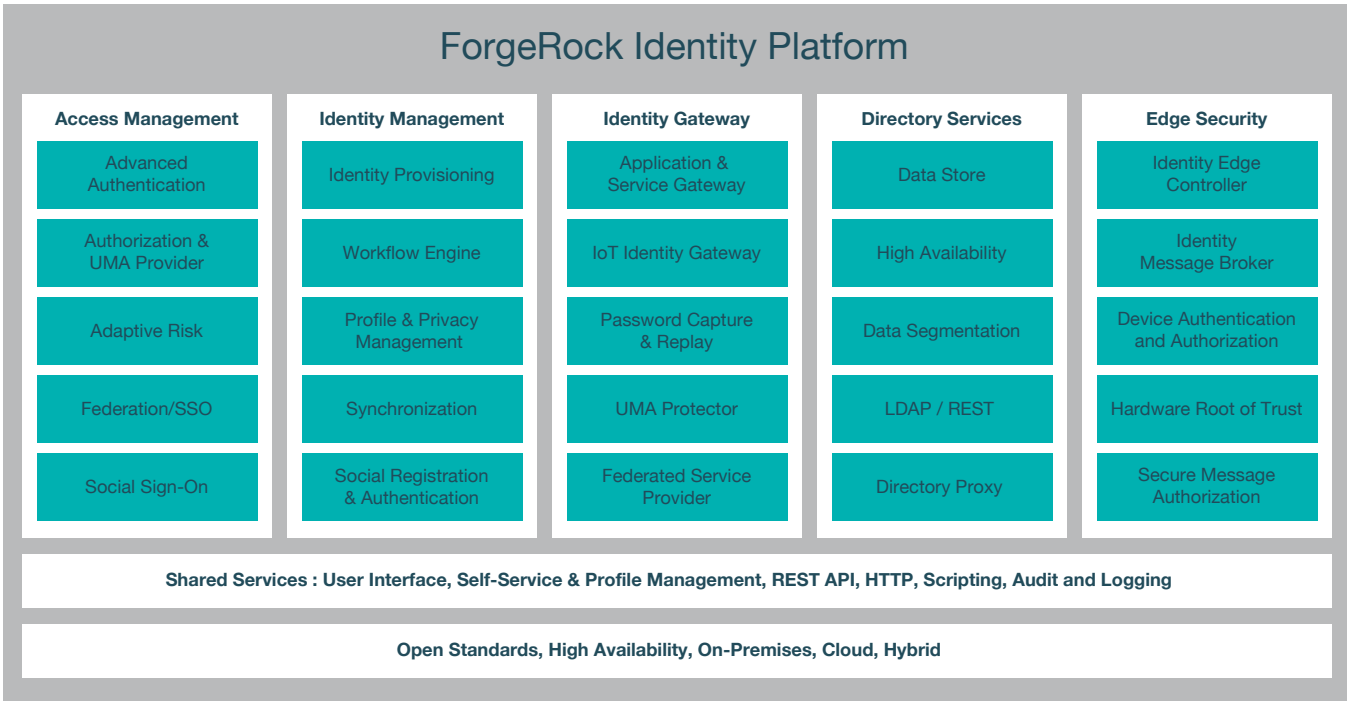
Avoid turning data into 'toxic waste'

Be aware that the use of 5G applications will generate massive amounts of data that, without appropriate management and controls, could compromise privacy regulations and undermine trust in the various ecosystem participants. Customer data have the potential to become 'toxic waste,' a huge liability for the CSP and other participants. Users must be able to control how their data are managed from the point of view of privacy and consent. Service providers should ask for only the minimum viable user profile required for service delivery. The CSP's trusted IDP service must extend privacy and consent controls to its users and enforce the user-defined sharing and control policies under its control.

> *Half of all respondents named bad UX as the number-one reason to lose trust in an app or service.*
>
> MEF MOBILE ECOSYSTEM FORUM

Work With ForgeRock to Deploy Network-Level Trust

The ForgeRock 5G Identity Relationship Management architecture is shown at a high level below, outlining how Identity is managed across the ecosystem, from service provider to endpoint device, and between devices within the IoT domain.



Becoming a trusted identity provider

A CSP should consider deploying its trusted IDP service in a carrier-grade cloud environment. The ForgeRock platform is architected and designed around carrier-grade scalability and rapid deployment in DevOps-driven environments and can be deployed using cloud, hybrid or on-premise patterns. Deploying to and integrating with PaaS platforms is a common theme enabled by our support for technologies such as Docker and Kubernetes. Access Management, Identity Management, Directory Services and Identity Gateway features are exposed through well-defined REST interfaces, enabling rapid integration with the CSP environment and the 5G ecosystem.

The ForgeRock Identity Platform is based on industry standards, leveraging protocols and standards such as OIDC, OAuth2 and UMA, enabling easy onboarding and integration of 5G network endpoints and third-party access within the 5G ecosystem. ForgeRock is also uniquely positioned for 5G applications with our investment in and innovation around on-device capabilities leveraging, for example, a trusted execution environment through the ForgeRock Identity Edge Controller and the ability to ingest sensor data through the ForgeRock Identity Message Broker. ForgeRock Identity Microservices provides a mechanism not only for identity-aware applications but also for exposure of CIAM services to 5G core platforms and 5G network slices.

> ***Key takeaway:***
> *CSPs, NEPs, application software providers, system integrators and device (small and large) manufacturers can all leverage ForgeRock capabilities for end-to-end application integration and deep integration into 5G platforms and associated ecosystems.*

Providing edge control in IoT

ForgeRock Edge Security, featuring the ForgeRock Identity Edge Controller and the ForgeRock Identity Message Broker, provides core capabilities for establishing trust in devices and data, and the secure transmission of events from network endpoints to 5G application platforms.

Leveraging standards such as OAuth2 proof-of-possession and integration in manufacturing and personalisation processes, the Identity Edge Controller will be able to facilitate securing and asserting device ownership, integrity and access.

> ***Key takeaway:***
> *The ForgeRock Identity Message Broker enables devices that cannot run a full HTTP stack to interact and integrate with 5G application platforms. Such constrained devices may use protocols such as MQTP and CoAP. They may be attached to IoT-optimised 5G network slices leveraging 5G New Radio (NR) and dedicated core network slices based on virtual network functions.*

Enabling privacy and consent management across IoT

CSPs sit on valuable digital information that other 5G ecosystem participants could leverage on a commercial basis. For example, the CSP will be able to provide asserted digital claims that other 5G ecosystem participants can trust and depend on.

The ForgeRock platform provides privacy and consent management features that enable CSPs to position themselves as trusted IDPs in the 5G ecosystem. Our support for core privacy and consent enabling standards such as UMA will allow CSPs to provide its users services for sharing, delegating, monitoring and managing user data.

Privacy and consent services will be integral for onboarding devices, then sharing data and access to the operations of those devices and how they integrate with 5G application service providers.

The ForgeRock platform provides end-to-end capabilities that will enable 5G applications to be rapidly onboarded and consumed. The applications will be able to explore the IRM features that expose how users, devices and services are interlinked and used.

CSPs leveraging the ForgeRock platform can provide UMA-based authorisation services and provide user-focused flows for onboarding devices using OAuth2 device flows in combination with UMA resource set registration flows.

The benefit to the user is that there will be a central privacy and consent (sharing) dashboard where the user can manage, for example, vehicles, a home security system or health data sharing. The benefit to the CSP is that it can offer UMA authorisation services to the wider 5G ecosystem, avoiding fragmentation in where and how the users have to manage privacy and consent interactions.

As CSPs also have access to a wide range of data relevant for contextual security, they are also well placed to enforce policies that apply to accessing shared data or controlling a device.

Such services and associated assertions provide a business opportunity for the CSP, which can charge a fee for taking on a level of risk associated with the assertion. In a GDPR environment, the relying parties (for example, the various 5G application service providers) will probably welcome not having to deal with a full set of PII and prefer to rely on assertions provided by another trusted provider.

CSPs, like financial institutions, are also often required to undertake Know Your Customer (KYC) processes, which further extend the value of the customer information they require and manage. As national identity ecosystems are emerging, a CSP can play a role in identity assurance. The ForgeRock platform is well suited for integration with, for example, biometrics-based enrollment and verification services, and the associated authentication and authorisation services.

> ***Key takeaway:***
> *By leveraging the core ForgeRock platform and our ecosystem of partners, a CSP can not only improve on existing IAM processes and user experiences but also build out new CIAM-based revenue streams that will power the 5G ecosystem.*

Conclusion

With the imminent launch of 5G, telecoms network operators have the tools and opportunity to become trusted identity providers as custodians not only of the identity of people but also of their devices and connected things in platform-based IoT ecosystems that they underpin.

With the right tools, 5G represents a new opportunity for network providers to re-invent themselves as globally trusted digital market participants. By offering trusted identity management at the network layer, they can become key enablers within digital ecosystems. They can provide the secure connectivity required to tap into the massive opportunity across multiple industry sectors presented by the billions of things with a digital heartbeat that will be powered by 5G networks, platforms and applications.

ForgeRock. Trust Conquers All.

Reluctant Sharers have been replaced by Savvy Consumers – smartphone users who jealously guard their privacy and security, but who at the same time reward trustworthy apps and services.

About ForgeRock

ForgeRock®, the leader in digital identity management, transforms how businesses build trusted relationships with people, services, and things. Organizations adopt the ForgeRock Identity Platform™ as their digital identity system of record to monetize customer relationships, address regulations for privacy and consent (GDPR, HIPAA, PSD2, Open Banking, etc), and leverage the internet of things. ForgeRock serves hundreds of brands, including Morningstar, Vodafone, GEICO, Toyota, TomTom, and Pearson, as well as governments like Norway, Canada, and Belgium, securing billions of identities worldwide. ForgeRock has offices across Europe, the USA, and Asia.

Get free downloads at www.forgerock.com and follow us @ForgeRock