Service Description

emnify GmbH

May 2, 2023

Version 1.2

Contents

1 Purpose of this document

This document outlines emnify's service offering for IoT solution providers who use emnify's cloud native IoT communication platform to bring their devices online, as well as integrate and manage global device connectivity. Throughout the document any of these types of customers are referenced as Enterprises.

The document outlines key service offerings, available functionalities of the emnify platform including private IoT networking, integration, and quota management, as well as emnify's customer support. emnify provides eSIMs that are built specifically for IoT solutions. Compared to regular operator SIMs, emnify eSIMs come in different quality grades that are more durable. They can be updated over the air (OTA) using different eSIM remote SIM provisioning technologies and come in different form factors.

2 emnify IoT eSIM

emnify eSIMs have a multi-IMSI applet installed on the SIM. The multi-IMSI applet makes sure that the best network and network partners are used based a device's location. Using this technology, emnify provides a larger number of networks than traditional operators. With access to the largest global LPWAN (LTE-M and NB-IoT) footprint, emnify SIMs ensure regulatory network access in over 100 countries.

2.1 eSIM technology

2.1.1 M2M eSIM

Every new SIM you order from emnify is an M2M eSIM (compliant with SGP.01, SGP.02, and SGP.016). The M2M eSIM is also referred to as an eUICC (Embedded universal integrated circuit card). Unlike a regular SIM (UICC), an eUICC can be updated over the air. Because M2M eSIMs can be updated with new configurations or profiles, this eliminates the need for SIM swaps.

2.1.2 Consumer eSIM

emnify also offers consumer eSIMs for phones, tablets, and smart watches. The consumer eSIM can be downloaded to a device by scanning a QR code. If you are interested in consumer eSIM technology, please contact us.

2.2 Form factors

emnify M2M eSIMs are available in the following form factors.

Form factor	Dimensions
2FF (Mini SIM)	15 x 25 x 0.75 mm
3FF (Micro SIM)	12 x 15 x 0.75 mm
4FF (Nano SIM)	8.8 x 12.3 x 0.75 mm
MFF2 (eSIM)	5 x 6 x 0.75 mm, 8 pin

MFF2 eSIMs can be soldered onto a device and are not readily removable. Visit the emnify SIM Shop where you can choose between these packages:

- Triple-cut commercial
  - Mini (2FF)
  - Micro (3FF)
  - Nano (4FF)
- Dual-cut commercial
  - Mini (2FF)
  - Micro (3FF)
- Single-cut Mini Industrial (2FF)
- Single-cut Micro Industrial (3FF)
- Embedded MFF2

In use cases where devices are mobile, we highly recommend choosing the form factor that fits the device exactly, not multi-cut ones that include a smaller form factor than is needed. Not only are such pluggable SIMs more durable, but their contact with the device is also firmer.

2.3 Quality Grades

emnify eSIMs come in three different quality grades: **Commercial eUICC**, **Industrial eUICC**, and **MFF2**.

		Commercial eUICC	Industrial eUICC	MFF2
Form Factor	Embedded/solderable	-	-	MFF2
	Removable Card	Triple-cut or Dual-Cut	2FF or 3FF	-
Chip Type	Operational and storage temperature	25°C to +85°C (JESD22-A104)	40°C to +105°C (JESD22-A104)	
	Operating voltage	1.62V to 5.5V		
	Interface	ISO-7816, T=0		
	Chipset NVM size	704 Kbytes		
	Chipset RAM size	20 Kbytes		
NVRAM characteristics	Write Endurance	500k erase per page 10M cycles with OS High Endurance		
	Data retention	15 years @ 85°C		
	Moisture/Reflow conditions	-	MSL3 (J-STD020)	
	Humidity	-	HA as per ETSI TS 102.671 / (JESD22-A101D)	
	Corrosion	-	-	CX as per ETSI TS 102.671 (JESD22-A107)
	Vibration	-	-	VX as per ETSI TS 102.671 (JESD22-B103)
	Shock	-	-	SX as per ETSI TS 102.671 (JESD22-B104)
	Common Criteria Certificate	CCN-CC-5/2019		

2.4 Compliance and software features

The following compliance standards and software features apply to all quality grades of emnify eSIMs.

emnify eUICC Compliance	GSMA	SGP.01 Embedded SIM Remote Provisioning Architecture	1.1
		SGP.02 Embedded UICC Technical Specification	3.2
		SGP.16 M2M Compliance Process	1.1
	TCA	eUICC Profile Package Interoperable Format Technical Specification	2.1
Software Features	Embedded Universal Integrated Circuit Card (eUICC)	Maximum number of profiles	10
		ISD-A and ISD-R system applets	Supported
		EAP-SIM and EAP-AKA authentication protocols	Supported
	LPWAN features	Suspend and resume SIM state ETSI TS 102 221 Poll Interval Negotiation ETSI TS 102 221	Supported
	OTA Capabilities on ISD-P: Remote file management – RFM Remote applet management – RAM	HTTPS	Supported
		TLS 1.2	Supported
		AES algorithm (128-bit, 192-bit, and 256-bit keys)	Supported
	GlobalPlatform	All Secure Channel Protocols	Supported
	Java Card	Standard Java Card APIs	Supported
		GlobalPlatform API	Supported
Compliance		ROHS	Yes
		REACH	Yes

2.5 Multi-IMSI applet

emnify eSIM cards are equipped with a multi-IMSI applet that runs in the background using minimal resources without any negative impact on the device's performance. This technology is similar to a mobile phone using dual-SIM technology. An emnify eSIM has cellular provider information from multiple SIM cards already included. While emnify has

roaming agreements and local contracts with operators around the world, emnify also uses partner operators to increase the network coverage footprint in order to provide a fallback when preferred networks experience outages.

The multi-IMSI applet works in the following manner. emnify has its own operator identity (IMSI) as well as the partner operator's IMSI stored on the SIM card. Each IMSI / partner operator usually has more than one network accessible per country. The applet also includes a preferred IMSI list per country. For example, this list defines that IMSI *X* will have the highest priority for access in country *A*. However, if the device can't connect, another operator, IMSI *Y*, will be next on the list of priorities. So when a device then moves to country *A*, the applet dynamically overwrites the active IMSI with IMSI *X* based on the preferred IMSI list. Then when operator *X* has a service outage, the SIM automatically falls back to IMSI *Y* to ensure the device can maintain connectivity.

The selection of the preferred IMSI for each country is based on multiple factors, including:

- If permanent roaming is permitted in that country
- IMSI that has the most network partners in the country
- IMSI that has the best availability of radio access types (LTE, NB-IoT, LTE-M) or features (PSM/eDRX)

3 emnify IoT SuperNetwork

3.1 emnify network coverage

Even when IoT devices are more often only deployed at a single location and are not moving, for a vendor selling to multiple countries it is important to have a global connectivity solution, so that there is no need to have different SIM cards in stock or have multiple contracts and tariffs.

3.1.1 Global coverage

emnify uses an approach to aggregate the roaming footprint of multiple operators with the goal of offering access to every network in the world. Mobile operators utilize roaming in foreign countries so their subscribers can stay connected when traveling. Often operators do not have roaming agreements with all countries or only have a roaming agreement for one network – which is sufficient for roaming travelers but not ideal for devices that could be anywhere in the country. emnify works with multiple partner operators across the globe to be able to offer more networks at a commercially viable rate. The emnify multi-IMSI applet makes it completely transparent for the device to identify which roaming agreement of which operator is being utilized.

3.1.2 Radio access types and frequency bands

The emnify IoT SIM and platform supports all devices and modules using the following radio access technologies

- 2G (GSM/GPRS/EDGE)
- 3G (UMTS/WCDMA/HPSA/HSDPA)
- 4G (LTE/LTE-A/LTE-CATXX)
- 5G (New Radio)
- LTE-M (CAT-M1)
- NB-IoT (CAT-NB1, CAT-NB2)

When a device wants to connect with any of these radio technologies, the network needs to support this technology as well as the device needs to support the network-specifc frequency band for this technology.

3.1.3 2G (GSM/GPRS/EDGE)

GSM/GPRS is still one of the most dominant IoT technologies. Although the throughput is limited (GPRS max. 120 kbps, EDGE max. 1 Mbps) it is more than sufficient for many IoT use cases. The modules are cheap (< $10) and the coverage is widely available throughout the world in more than 200 countries.

GSM/GPRS is easy to deploy for IoT use cases because there are only 4 frequency bands utilized by operators for GSM/GPRS worldwide.

In the Americas

- B2 (1900MHz)
- B5 (850MHz)

In the rest of world

- B3 (1800MHz)
- B8 (900MHz)

Therefore, module manufacturers offer dual-band modules that can be used either in Americas or Rest of World – or Quadband modules that can be deployed globally.

Nevertheless, GSM/GPRS is being phased out in several countries to free up frequency band for newer technologies. More than 60 networks have discontinued or announced to discontinue GSM technology.

3.1.4 3G (UMTS/WCDMA/HPSA/HSDPA)

3G technologies like UMTS, WCDMA, HSDPA, HSUPA have been driven by the surge for more data speed. As an evolution of GSM, many parts of the GSM/GPRS core network and signaling are reused, where the most difference is in the radio part.

Like 2G, 3G modules are easy to deploy, since there are only 5 different frequency bands utilized by operators worldwide (with exception of Japan and China). Most UMTS modules therefore can be deployed worldwide.

- B1 (2100MHz) - main UMTS band in the world
- B2 (1900MHz) - used in the Americas
- B4 (1700MHz) - used in the Americas
- B5 (850MHz) - Australia / the Americas
- B8 (900MHz) - Europe

For Europe, a 900/2100 MHz dual-band module is required. For the Americas a 850/1900 MHz dual-band module is required.

3G/UMTS is also being phased out by several network operators to make room for newer technologies. See also the article on GMS and UMTS networks that are being discontinued

3.1.5 4G (LTE/LTE-A/LTE-CATXX)

LTE is a 4G technology (another one would be WiMAX – which never succeeded). With the evolution of LTE, various LTE categories have been established, such as CAT-1, CAT-3, CAT-4, CAT-6, CAT-9, and CAT-12 Each successive category has exhibited ever-increasing data throughput when compared to its predecessors. For consumer phones and broadband use cases, the increased throughput is relevant. However, the increased costs for these modules resulted in the need to develop a lightweight LTE module for IoT use cases. In turn, this led to CAT-1 as the preferred LTE category for IoT applications.

LTE CAT-1 offers 10 Mbps in downlink, 5 Mbps in uplink, and is available with network operators wherever LTE is deployed. Because of its wide availability and the possibility to roam between operators without limitation, LTE CAT-1 is the most common choice for IoT use cases.

Deploying LTE devices on a global scale is more challenging than with GSM and UMTS because network operators worldwide use more than 27 different frequency bands. Therefore, most modules only support specific regions where the device can be deployed.

Some main LTE-bands are

- B3 (1800 MHz) - Europe, Africa, APAC
- B7 (2600 MHz) - used in the Americas, Europe, APAC
- B20 (800 MHz) - used in Europe, Asia
- B1 (2100 MHz) - Europe, Asia
- B2 (1900 MHz) - the Americas
- B4 (1700 MHz) - the Americas
- B5 (850 MHz) - North America, APAC

Tip

Validate the frequency bands utilized by the operators in your deployment countries before deciding on a module.

3.1.6 LPWAN: LTE-M/NB-IoT

While utilizing LTE infrastructure both NB-IoT and LTE-M are also part of the 5G standardization. Both technologies have been specified to meet the demand for IoT use cases in terms of:

- Reduced cost – to enable mass production of cellular IoT devices
  - Removing unnecessary LTE features for IoT such as dual carrier, high modulations
- Low power utilization – for battery powered use cases that require years of operation
  - Introducing power saving features such as PSM and eDRX
  - Reducing the max. transmission power to less than 200mA to cater for battery max. current (GSM for example has 2A max power)
- Wider coverage – (+14 dB for LTE-M and +20 dB for NB-IoT sensitivity) for rural/indoor/underground use cases
  - Utilizing extended coverage feature with more retransmissions to ensure data gets delivered
- Smaller module size – to enable smaller device use cases

Because LTE-M and NB-IoT rely on LTE infrastructure they are also deployed in a multitude of different frequency bands. A total of 26 bands have been specified for their use. To deploy NB-IoT and LTE-M in multiple countries and regions, the modules need to support the operator frequency bands.

Cellular LPWAN modules come in different versions

- NB-IoT only or LTE-M only
- LTE-M/NB-IoT combined

- LTE-M/NB-IoT with 2G fallback and optional additional technologies (3G, 4G)

As of today, roaming for NB-IoT is very limited between operators because of new charging models being implemented for NB-IoT. For LTE-M, roaming usually works over regular LTE roaming. Nevertheless, some operators have limited the access to their LTE-M networks and its available features (PSM, eDRX).

Check the emnify LTE-M coverage and NB-IoT coverage, availability of PSM/eDRX and proposed frequency bands on our Website.

Power-Save-Mode (PSM)

- Why is cellular communication not ideal for IoT? Cellular communication for smartphones usually requires low latency on downlink, e.g., in case you are being called, your phone should ring right away. Because of this, there are two things the device does which require power:

1. Continuously listening to the radio if there is an incoming call
2. Transmitting location information to the network where it should be called – whenever it moves out of a tracking area and periodically every 54 minutes

- How does **Power Save Mode** work?

For most IoT use cases a downlink-initiated channel is not required. It is usually the device that initiates the communication to send e.g., sensor data. Therefore, a **Power Save Mode** is introduced that allows the device to go to sleep in case it has nothing to send.The **Power Save Mode** has the following characteristics:

- The Power Save Mode is like a power off period during which the module only consumes a couple of A.
- The device tells the network how long it is going periodically into PSM (timer T3412 extended).
- The device/module will not be reachable during PSM from the outside in downlink.
- The device can wake up the module and send data (e.g., powerkey, interrupt or pin triggered).
- When the device wakes up, it does not need to reattach and re-establish a PDN connection (unless it has moved to a different tracking area).
- After the device wakes up, it stays in idle mode for a configurable time (timer T3324) to listen for downlink messages (e.g., firmware updates).
- The actual time the device is then in Power Save Mode is T3412 extended – T3324

Note

Some modules which have a SIM enabled PIN, (e.g., u-blox SARA-R4/SARA-N4) do not go into sleep mode. The PIN is disabled on emnify SIMs.

- Roaming for Power Save Mode

Be aware that not all NB-IoT and LTE-M networks have implemented PSM and even when PSM is available with the local operator this does not mean that a roaming SIM can use it. This makes it difficult for devices that are moving – in case they use PSM, and the new network does not support PSM – or only other timer configurations. We therefore regularly test the availability of PSM in our LTE-M and NB-IoT roaming footprint.

- AT Command calculation and examples for PSM settings

The 3GPP defined AT command to configure PSM is `AT+CPSMS` which sets the T3412 extended and T3324 timers.

An example command is

```
AT+CPSMS=1,,,01001110,00000101
```

PSM will be enabled (`1`) and the desired value for T3412 extended is 140 hours (`01001110`) and the desired value for the T3324 timer is 10s (`01001110`). The network does not necessarily use the desired values but utilizes supported values that are close to the desired values. To read the effective PSM configuration use the command

```
AT+CPSMS?
```

There is a good calculator that translates the intended time settings for 3412 and T3324 available from Thales.

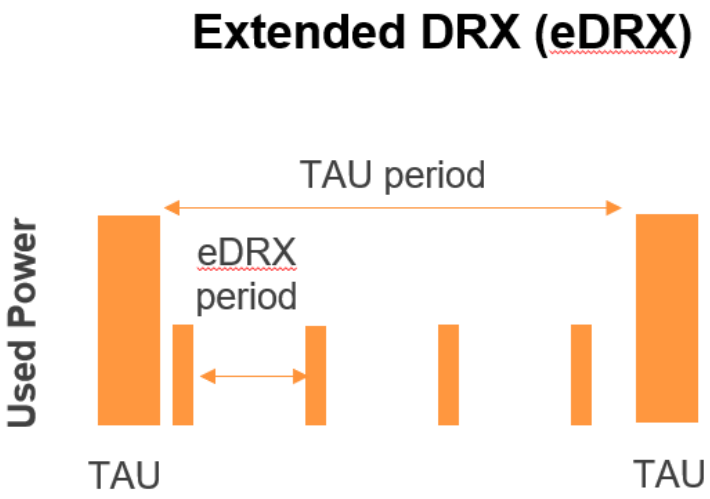
Module vendors have also implemented module specific commands, e.g. Quectel

- `AT+QPSMS` extends PSM settings
- `AT+QCFG="psm/enter",1` used to put the module immediately into PSM when the RRC connection is released (not waiting for T3324 to expire)
- `AT+QPSMEXTCFG` modem optimization command with different attributes such as making sure that PSM is randomized between different devices so they do not send data at the same time

Extended Discontinuous Reception (eDRX)

- How does eDRX work?

While PSM is focused on uplink-centric use cases, eDRX tries to reduce the power consumption for IoT use cases that get downlink information. Regular smartphones do not continuously listen on the radio for an incoming message. They do this only every 1.28s or 2.56s which is called DRX (discontinuous Reception). eDRX allows configuration of custom intervals of up to 40-175 mins – depending on the configuration the visited network allows.



- Roaming with eDRX

As with PSM – not all NB-IoT and LTE-M networks support eDRX or the same timer configuration – and even if they do this does not guarantee that a roaming SIM card can utilize eDRX. We therefore also test and publish the eDRX availability on our LTE-M and NB-IoT roaming footprint.

- AT Command examples for eDRX settings

The standard 3GPP defined AT-command to configure eDRX is `AT+CEDRXS`.As an example the below command enables (`1`) eDRX for LTE-M (`4`) and an eDRX cycle of 143.36s (`1000`).`AT+CEDRXS=1,4,"1000"`

The setting for NB-IoT would be `5` and the timer values are shown in below table

Binary	Timer Value
0 0 0 0	5.12 seconds
0 0 0 1	10.24 seconds
0 0 1 0	20.48 seconds
0 0 1 1	40.96 seconds
0 1 0 0	61.44 seconds
0 1 0 1	81.92 seconds
0 1 1 0	102.40 seconds
0 1 1 1	122.88 seconds
1 0 0 0	143.36 seconds
1 0 0 1	163.84 seconds
1 0 1 0	327.68 seconds
1 0 1 1	655.36 seconds
1 1 0 0	1310.72 seconds
1 1 0 1	2621.44 seconds
1 1 1 0	5242.88 seconds
1 1 1 1	10485.76 seconds

The network will respond with the actual effective interval.

```
+CEDRXS: [4,"1000","1000","0111"]
```

3.1.7 5G (New Radio)

5G is the next major technology standard after LTE – which targets 3 different applications areas:

1. Enhanced Mobile Broadband (eMBB)
   - With faster throughput upto 1Gps+ and more capacity in a local area
   - Utilizing mmWave bands (5Ghz+) for increased throughput
2. Massive Machine Type communication (mMTC)
   - Targeted at IoT application where a multitude of devices are in the same location and need to communicate with low power
   - LTE-M and NB-IoT often seen as decoupled from 5G to get earlier results will fusion with 5G mMTC
3. Ultra-Reliable Low Latency Communications (URLLC)

- For missing critical applications that require low latency and reliable data transmission

As of today, 5G is mainly adopted for eMBB use cases – using a 5G non-standalone (NSA) deployment – meaning that the air interface uses 5G technology whereas the core network is still 4G.

emnify has announced its first 5G roaming agreements in August 2020 and since then has reached agreements with more than a dozen network operators worldwide.

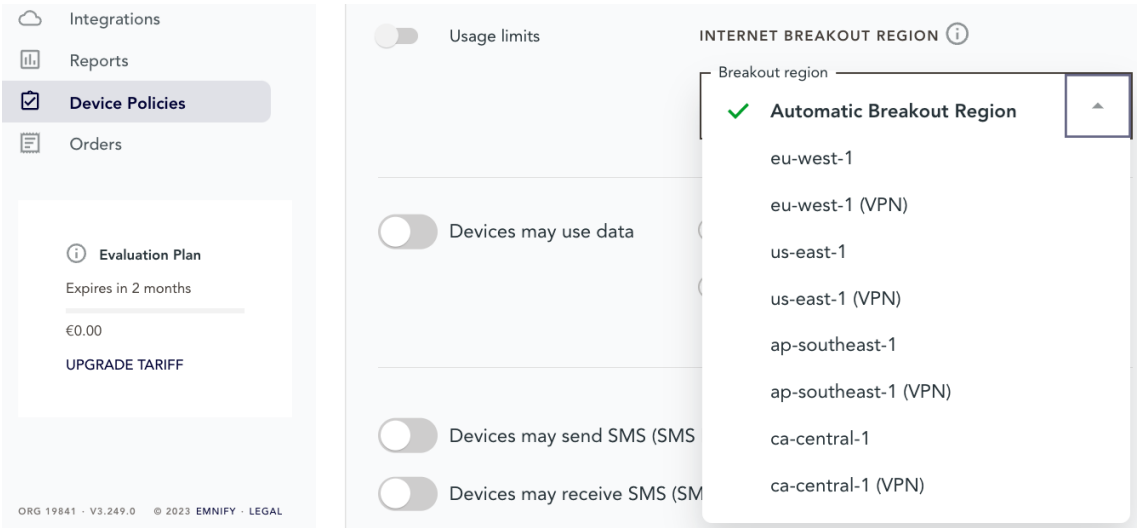
3.2 emnify local connectivity

3.2.1 Traditional home-routing vs regional breakout

The data plane of emnify's cloud communication platform is distributed across major cloud regions (Virginia/US, Ireland/Europe, Singapore/APAC) and directly connected to central peering points with the local operators.

3.2.2 emnify regional breakouts

emnify's distributed data plane enables device data to breakout locally, keeping the customer data within the same region. Moreover, it also helps reduce network latency. You can either select a specific breakout region or the network automatically selects the breakout region closest to the device. This can be done on the emnify Portal » **Device Policies** » **New service policy** which is applicable to a group of devices.



4 emnify connectivity platform

emnify's connectivity platform provides solutions for configuring, deploying, maintaining and monitoring your IoT assets globally. It it comprised of the following set of of tools.

4.1 emnify Portal

The web-based emnify Portal is the starting point for signing up and ordering your global IoT eSIMs. It is where you can create service and coverage policies for your IoT devices. Almost every aspect of your IoT network can be managed within the emnify Portal, including integrations with third-party solutions.

4.1.1 Operation Center

- Dashboards
- Device details
- Location Information
- Network reset

4.1.2 SIM management

- Ordering SIMs
- SIM lifecycle management

4.1.3 User and Account Management

- Single-Sign On
- Multi-Factor Authentication
- User Roles
- Workspaces

4.2 emnify APIs

4.2.1 REST API

REST APIs are one way to integrate external services into your application. The emnify API provides a variety of HTTP requests to integrate several emnify services into your application.

The emnify API is based on the OpenAPI Specification OAS3.

4.2.2 GraphQL

GraphQL is a query language that enables you to define API call responses to match your use case and technical needs.

The emnify GraphQL API was initially developed internally to improve performance on the Portal. In early 2023, we decided to release a preview version to customers. We hope to collect feedback and continue adding features so that the functionality more closely matches our REST API.

4.2.3 Data Streamer

With the emnify Data Streamer, enterprises can integrate real-time connectivity data directly into their third-party cloud services or business systems to build operational dashboards that visualize device, network, and application information side-by-side. With this comprehensive view of their IoT solution and infrastructure connectivity data, they can quickly triage and resolve issues or create business reports.

4.2.4 SDK

The emnify software development kits (SDKs) allow developers to manage their IoT devices using an intuitive set of APIs, including SIM state management and device connectivity operations. emnify SDKs are currently available for Java and Python.

4.2.5 No-Code

Zapier is a service that allows you to connect more than 4,000 applications – including emnify – to automate workflows. With the available integrations you can automate device provisioning between emnify and your application. For example, you can send configuration SMS to set the proper APN, when the device connects for the first time. Other use cases are scheduled or application-triggered SIM activations/deactivations so that the SIM contract starts and ends with the device subscription of your customers. The following events are available as triggers:

- All events in the Data Streamer
- Device enabled (SIM activated)
- Device disabled (SIM deactivated)
- Usage Limit Reached

The following actions are available:

- Send SMS to device
- Create a device (SIM configuration)
- Enable a device (SIM activation)

- Block current network (blacklist the last tried network)

Using the Zapier webhook, you can also use triggers from:

- SMS delivered notification
- Mobile originated (MO) SMS

4.2.6 Events

The emnify system generates several types of events. These events allow you to track notable system occurrences based on behavior.

Some common use cases for events on emnify include:

- **Triggers for custom business processes** (e.g., authentication or custom usage limitations configured on the emnify Portal)
- **Monitoring** (e.g., SIM or data connection lifecycles)
- **Input for custom billing systems** (i.e., updating billing configuration, processing invoices, etc.)

Events are often used as triggers for custom business processes, for monitoring, and as input for custom billing systems. They provide information about lifecycle transitions and configuration changes.

5 Communication services

5.1 Data

5.1.1 Public internet breakout

An internet breakout is where data passes from a private network to the public internet. For cellular networks the internet breakout is the home operator's central location – the one that sold the SIM card. This can pose a challenge for organizations with globally distributed devices. Data might have to be routed through multiple countries or even across continents before arriving at the home operator's centralized data center before being sent to its final destination.

5.1.2 Virtual Private Network

Private APN

A private Access Point Name (APN) is a solution that was developed to simply identify a gateway having specific policies for accessing a network that assigns static IP addresses to devices through which they can be remotely accessed. The private APN was then used as an concentrated endpoint to help secure connectivity through policies like blocking public internet access. Private APNs are often used in conjunction with a VPN. However, emnify doesn't require a private APN for using a VPN.

OpenVPN

emnify's communication platform hosts an OpenVPN service that allows you to establish a private network between a device and any remote client location. The remote client can be on the application server or any machine that wants to access the device remotely (such as operational staff).

Your IoT device doesn't need a private APN, OpenVPN software, or dynamic DNS resolution to use the OpenVPN service. Through the emnify IoT eSIM, each device will have a static private IP address that you can use to identify and address the device.

At the same time, the IoT device can send data through the private tunnel to the IP address of the remote machine.

Cloud Connect

The data traffic of regular SIM cards is secured within the mobile network – but traverses the public internet between the mobile network and the application, which makes the device and application susceptible to attacks and prohibits to easily establish a remote device session.

With emnify Cloud Connect your devices and application servers can communicate through a secure private network – with a secure tunnel being established between the emnify platform and your cloud or on-premises application.

By eliminating the use of the public internet, Cloud Connect helps you better protect your application infrastructure against attacks like DDoS, port scanning while giving you the possibility to remotely access the devices.

5.1.3 Inter-device communication

Traditionally, short message service center (SMSC) facilitates short message service (SMS) communications between devices on the network. Text messaging and many Internet of Things applications depend on SMSCs to relay communications from one device to another. In order to communicate with a network's SMSC, you'll need to enable your application to use Short Message Peer-to-Peer Protocol (SMPP). This is a complex protocol that can be difficult to work with.

At emnify, we simplify SMS communication with our RESTful API. This enables your devices to communicate over SMS using JavaScript Object Notation (JSON), and you don't have to worry about SMPP.

5.1.4 Regional breakout

A regional internet breakout is when a distributed network routes data through regional data centers, typically through cloud service providers like Amazon AWS, Microsoft Azure, or Google Cloud.

emnify uses AWS to facilitate dynamic regional internet breakout to dynamically select the closest breakout region based on a device's location while using other availability zones as backups to prevent downtime.

5.2 SMS

SMS messages can play a pivotal role in remote IoT device management and automation. Since SMS works without a data connection, it's a reliable way to communicate with remote IoT devices.

By designing devices to accept SMS parameters, most manufacturers have eased the burden of configuring a fleet of devices, both for the initial connectivity configuration as well as for post-deployment configuration changes.

By leveraging SMS for specific tasks that would overwise require power-hungry data connections, devices can operate more efficiently by conserving battery power.

With SMS in place for your remote configuration, you can also use it to trigger additional actions on a device. For example, if you wanted to perform an update, you could use SMS to trigger a firmware OTA update.

5.2.1 SMS MO/MT

The ability to send and receive point-to-pont (P2P) SMS messages is often abbreviated as follows:

- **MO** Mobile-Originated, i.e., messages can originate (be sent) from this device
- **MT** Mobile-Terminated, i.e., messages can terminate (be received) at this device

5.2.2 P2P SMS

Some countries implement a strict interpretation regarding what constitutes person-to-person (P2P) SMS communication. In such cases, any application-mediated messaging is considered A2P instead, even if the originator and recipient are both non-commercial, individual consumers.

emnnify allows MO and MT SMS from external SMS devices. Devices can be reached over the assigned MSISDN number from any regular mobile phone.

5.2.3 A2P SMS

Application-to-Person (A2P) Short Message Service (SMS) refers to text messages sent from a software program to person or a SMS sent from a person to an application. Messages from an application are often automated and trigger based on a set of rules or conditions. Messages to an application involve a request or command.

In the Internet of Things (IoT), end users and manufacturers rely on A2P SMS to do things like remotely set the Access Point Name (APN), reconfigure devices, "wake up" a device to go online, or send small measurement data to the application.

Note

A2P and P2P Routing
emnify distinguishes A2P SMS from P2P SMS based on the length of the source or the destination address.
If there are 8 digits or less (i.e., an invalid MSISDN), an SMS will be considered A2P.
If there are 9 digits or more, an SMS will be processed as MSISDN and will be considered P2P.
To dispatch SMS MO to your application and at the same time have P2P SMS enabled, the destination number must be limited to 8 digits or less.

SMPP

Short Message Peer-to-Peer Protocol (SMPP) is the system of rules that lets devices and software applications send and receive text messages over the internet. Cellular Internet

of Things (IoT) devices such as smart meters use the SMPP to transmit updates about resource consumption and location status. When an event like a break-in or fire triggers a smart alarm system, it uses the SMPP to message the building owner, potentially with a link that allows them to access a camera feed.

SMS via the emnify REST API

If you're an IoT manufacturer, your device may rely on SMS communication. In these cases, emnify can automate your SMS data exchange between device and application through the REST-API. The REST-API does not only allow to programmatically send SMS to the device but also to retrieve the SMS data the device sends.

SMS console in the emnify Portal

The emnify Portal also provides an SMS console which allows an SMS to be sent to the device with a configurable source address. In addition, the UI lists all SMSs that are received and sent by the device.

5.2.4 SMS short codes

SMS short codes are often associated with automated services, each of which is assigned a unique short code and phone number. Within the emnify core network, there is no SMS short code configuration required per specific customer or service. All SMS messages that are sent and received from a specific customer will be forwarded through the API or SMPP. This means each customer can use their own short codes and customize them based on their use cases.

6 Network security services

Given the globally distributed nature of the devices, smaller footprints and lack of resources, it can get difficult to individually secure IoT devices.

emnify uses a SASE approach to simplify securing devices – using several services specifically to protect customer data, filtering malicious content and preventing unauthorized access.

6.1 SASE overview

Secure Access Service Edge (SASE) introduces a new architecture where networking and security functions are bundled in a cloud-delivered service. You can apply the same security standards across all your devices independent of the location. Moreover, you can integrate security features in your solutions right from the beginning.

Some of the features that SASE for IoT architecture includes are as follows:

- Dynamic Data Routing with Software-Defined Wide Area Network (SD-WAN) emnify utilizes a SD-WAN to route data to the closest cloud region using the Regional Breakout concept. In this way, latency and data stability is improved, and the end customer can be sure that data does not leave the continent and jurisdiction.
- Cloud Access Security Broker (CASB) emnify allows centrally defining policies for the devices such as: networks that can be accessed, allowed IP addresses through which authorized users can remotely access devices. All configuration is done in the central platform and applied wherever the device is.

6.2 Virtual Private Network options

A Virtual Private Network (VPN) enables encrypted, targeted transmission of data over public networks such as the internet. It establishes protected and self-contained networks with various devices. A common use case is the connection of home offices or mobile employees.

6.2.1 Private static IP

Assigning a device a private static IP address prevents computers or other devices outside the local network from directly connecting to it.

6.2.2 Cloud Connect – secure data transport

AWS Transit Gateway

Connect devices securely to AWS VPC without using public Internet. Some of the features and benefits are:

- Devices and the application infrastructure reside within the same private network.
- Remotely access devices from AWS infrastructure via telnet / SSH.
- Device data does not traverse public internet.
- VPC / EC2 instances do not need public IP addresses.
- Fully scalable and managed AWS service.

IPsec

If your application is not on AWS but on any other cloud services or on-premise, you can utilize Cloud Connect for establishing an IPsec VPN connection.

With emnify you can set up an IPsec tunnel to securely transfer your data into your application server.

6.2.3 OpenVPN – remote access

OpenVPN is provided as a self-service for enterprise customers to get remote access to their devices from any OpenVPN client. Customer VPN clients are authenticated with the credentials and application tokens of their emnify account to get remote access to devices. OpenVPN establishes a single tunnel to the VPN gateways which are delivered in active-passive redundancy with automatic failover in case one VPN gateway becomes unavailable.

6.3 Custom DNS

When a device establishes a connection, it uses a Domain Name Service (DNS) server to resolve a hostname to an IP address to which it can send data. For example, a hostname such as `iot.example.com` will be mapped to an IP address like `192.0.2.1`.

Cellular providers typically provide a DNS service. By default, emnify routes all DNS queries over Google's public DNS `8.8.8.8`.

For some devices and modules, it is possible to configure the DNS service. For example, Quectel uses the `AT+QIDNSCFG` command, SIMcom `AT+CDNSCFG` command. This is useful to be able to use your own or private DNS servers to secure and have better control over the solution.

Customers can also configure to use their own DNS, no matter if it is a public or a private one. The DNS settings can be changed in the emnify Portal » **Device Policies** » **New service policy** » **More options**

Utilizing a private DNS server which is not reachable via the public internet requires to set up a private network with the machine or a network where the private DNS server is located. This can be done using Cloud Connect either with Amazon Transit Gateway or IPsec. A tutorial on how to set up a DNS firewall based on a private DNS using Amazon Route 53 is available here.

6.4 IMEI lock

For device manufacturers, SIM card theft is an issue because pluggable SIM cards can be removed from a device and then used to gain free internet access. The IMEI lock feature prevents the use of SIM card in any other device by bounding the SIM to an IMEI. The IMEI is a unique device identifier. When the automatic IMEI lock is configured, the emnify platform will bind the SIM cards to the first device that establishes a data connection. All future device connections will only be allowed from this device.

6.5 Centralized policies

Within the emnify platform, there is a separation between SIM card and the device, also referred to as "endpoint". This allows you to configure policies on the device level rather

than SIM level. The device policies can be applied on a device group as well as at an individual level.

6.5.1 Service policies

Service policies define which services are available for a group of devices. These policies include:

- Available radio access types (2G, 3G, 4G, NB-IoT)
- Monthly data and SMS limit
- SMS API configuration
- Custom DNS
- Breakout Region
- Available SMS service (MO/MT/P2P/A2P)
- Activation of Quota and Prepaid Management

6.5.2 Coverage policies

Coverage policies define which tariff and network coverage is available for a group of devices. This enables you to optimize the tariff based on the intended coverage.

The coverage policies include:

- The applied tariff for the group of devices
- The available networks organized in rate zones

7 Support

emnify is dedicated to your success with our service. We provide you with a choice of different plans, a globally-based customer success team, and support with global roaming to ensure that you have connectivity wherever you need it.

7.1 Service Options

emnify offers a variety of support plans designed to ensure that your devices operate reliably in our network. The **Standard** support plan is included for all customers at no additional cost. It is the default service plan when registering through our website using the emnify Portal. For a detailed description of the standard services, please refer to our Terms of Service.

The **Business** and **Enterprise** plans offer premium customer service and can be bundled with your emnify subscription. They are designed to reduce operational costs by detecting issues before they disrupt your business operations and by resolving incidents faster.

Feature	Standard	Business	Enterprise
Operating hours	Mon-Fri 09:00-18:00 CET	24x7x365	24x7x365
Method of contact	Tickets must be opened via webform. Replies via email are possible.	Ticketsmust be opened via webform. Replies via email are possible.	Webform, email, and phone
Help Center & Knowledge Base	Yes	Yes	Yes
Pre-scheduled event support	Not included	Yes	Yes
Dedicated Support Agent	Not included	Not included	Yes (EU-CET, US-EST or US-PST business hours)
Trace requests	–	1 simultaneous trace Max 1 request/day Max duration 24 hours/trace	3 simultaneous traces Max 1 request/day Max duration 24 hours/trace
Guaranteed response times: **Critical incident** **Operational incident** **General issue / question**	7 business days	3 hours, 24x7x365 6 business hours 9 business hours	1 hour, 24x7x365 3 hours, 24x7x365 6 business hours
Target time to restore service: **Critical incident** **Operational incident**	–	12 hours 10 business days	4 hours 4 business days
SLO	Mobile Core: 98.5% Internet Breakout/VPN: 98.5% API/GUI: 98.5%	Mobile Core: 99.5% Internet Breakout/VPN: 99.5% API/GUI: 99.5%	Mobile Core: 99.95% Internet Breakout/VPN: 99.9% API/GUI: 99.5%
Root cause analysis	Yes (Critical incidents)	Yes (Critical incidents)	Yes (Critical and operational incidents)
Length of service	Monthly (automatic renewal)	Monthly (automatic renewal)	Minimum 12 months

7.2 Incident Management

emnify's network operation center (NOC) monitors the health of all cellular networks and services that emnify offers 24x7. The NOC proactively identifies any degradation of service. In case of an incident, it starts the incident management process that alerts a team of on-call engineers to start an investigation.

When an incident is triggered due to network-related events, the responding team will diagnose the fault and escalate the incident to emnify's carrier and roaming partners if necessary. Optionally, any network causing a service disruption will be blocked so that devices can connect to alternate networks.

During an incident, emnify updates the Status page for all services in order keep customers informed in real time about the status of the incident and its impact.

For critical and operational incidents, emnify conducts a root cause analysis (RCA) and issues a postmortem that provides details about the incident, which changes have been applied, and which measures are planned to guard against future incidents.

The incident management process is reviewed annually and certified by a third party as part of emnify's SOC2 audit.

7.3 Roaming

Unlike typical mobile network operators (MNOs), emnify will also provide 24/7 support when your device is in roaming scenarios. The emnify network operation center (NOC) has visibility of all networks in the world and can detect network service degradation. emnify will also investigate and follow up even when only your fleet of devices is affected.

Based on the direct and IoT/M2M specific roaming relationships with network operators, emnify has service-level agreements (SLAs) to resolve critical and operational incidents within specific timelines.

So you will never need to worry about roaming when your IoT devices are moved to another location, even if it is to another country or continent. Support for the global deployment of IoT devices is a key feature of emnify's Global IoT Network.

7.4 Customer Success Manager

In addition to emnify's 24x7 support and network operation center (NOC), each customer has access to a Customer Success Manager (CSM). CSMs comprise a globally distributed team with local working hours. They are fluent in emnify's main supported languages: English, Spanish, Italian, French, and German. The CSM team proactively engages with their customers to help them obtain value from the product and guide them through their journey. They also conduct onboardings to get their customers acquainted with the platform and help with setting up integrations.