About eSim cards

tonisoft #1 27 July 2023 13:38

Hello, is anyone interested in an eSIM? Can we generate a QR code and use an eSIM with our BTS? The reverse option is also interesting, can we “pour” an operator eSIM into a sysmoISIM-SJA2 SIM type card? Also useful documentation related to the topic, and why not some FOSS project.

laforge #2 27 July 2023 14:16

> tonisoft:
>
> Hello, is anyone interested in an eSIM?

I guess many people are interested 🙂 - particulary I am, as well as (at least) lynxis.

> tonisoft:
>
> Can we generate a QR code and use an eSIM with our BTS?

The topic is rather complex. There is

1. The *technical* capabilities. This means having an eUICC and a UE with LPA.
2. Participation in the GSMA eSIM PKI (publickey infrastructure).

If you participate in the GSMA eSIM PKI, that means only a GSMA member mobile operator can create + sign eSIM profiles which can be installed on eUICC that are signed by a GSMA key. Both the eSIM profile is signed by a GSMA PKI-derived key, as well as the eUICC. You can do this either with a UE that hasa built-in eSIM or with any UE and a plastic SIM card sized eUICC like those of **esim.me**.

All you need is to have internet connectivity from your private network, and some kind of initial profile on the card that can join your network. You could also work around the latter part by not doing GSM authentication + encryption in your private network.

However, it will not be very interesting in terms of the eSIM profiles you can install: All of those are built to be used with commercial operators, and you won’t get to know the K/OPc or OTA key materials for those profiles.

On the other hand, it would be possible to operate a different PKI/CA than the GSMA production one. If you had the following parts:

- an eUICC with the certificate of that private PKI/CA
- an eSIM profile with a certificate of that private PKI/CA
- a SM-DP+ and SM-SR software implementation

then you would be able to install your own eSIM profiles (with known K/OP/OPc/OTA-keys) on your own eUICC and use those for example in your private, stand-alone network. The disadvantage is that you *must* use your own non-production eUICCs and cannot use any that have certificates issued by the GSMA PKI/CA. This means you cannot use a regular smart phone with built-in eUICC, as this will have a GSMA PKI/CA certificate, and not yours.

sysmocom could source and sell eUICCs with non-standard/private PKI/CA certificates, it has been something I have thought about for a long time. The problem is that without an open source SM-DP+/SM-SR, almost nobody would be able to use it.

> tonisoft:
>
> The reverse option is also interesting, can we “pour” an operator eSIM into a sysmoISIM-SJA2 SIM type card?

No, you cannot. The sysmoISIM-SJA2 is a UICC+USIM+ISIM+SIM card. It is not an eUICC. You would need an eUICC with GSMA certificate in order to participate in the production eSIM universe and install production operator eSIMs. In this case (obviously) everything is locked down and you would never know the K/OP/OPc/OTA-keys etc. of the eSIM profile you installed on that eUICC.

> tonisoft:
>
> Also useful documentation related to the topic, and why not some FOSS project.

Sorry, but this sounds a bit like *I want it all but not invest my time in actually writing that documentation or the FOSS*. That’s not how it works. The existing Osmocom developers/contributors have by now invested decades of person-years of R&D on cellular technology and released all of it as FOSS. But it is a wide field, from SIM cards to RAN to CN, from 2G to 4G or even 5G, so we can only do so much.

We do however welcome anyone wanting to contribute e.g. eUICC/eSIM support to pySim. We also welcome anyone wanting to present on the topic for example in an **OsmoDevCall**

Manawyrm #3 28 July 2023 07:19

> laforge:
>
> I guess many people are interested 🙂

Yup… I know that I’ve seen a talk by you somewhere (already a long while ago, might even have been at a real-life conference), where you talked in detail about eSIMs and the challenges involved (like the PKI).
If you know which talk that was, maybe you could/should share a link to a recording of it, I think it was quite interesting.

---

laforge #4 28 July 2023 08:52

> Manawyrm:
>
> I know that I've seen a talk by you somewhere (already a long while ago, might even have been at a real-life conference), where you talked in detail about eSIMs and the challenges involved (like the PKI).
> If you know which talk that was, maybe you could/should share a link to a recording of it, I think it was quite interesting.

I guess it was part of the "SIM card technology from A-Z talk" I gave at the last CCC Congress towards the end at **media.ccc.de - SIM card technology from A-Z**

Also note that I'm going to give a talk specifically about GSM eSIM at the upcoming Chaos Communication Camp 2023. There's no schedule/fahrplan yet available, but the talk was approved.

---

domi #5 28 July 2023 09:02

Just a small addition: in real life operators don't really bother with having their own SM-DP+, or signing profiles. It is all outsourced to SIM vendors, and basically from the operator's point of view there is no difference in eSIM or regular SIM. They place the order, provide the profile they want, and then the SIM vendor fulfills it.
This means most SM-DP+ around the world are shared between multiple operators. Also it is much easier for SIM vendors to satisfy requirements (compliancy, certification etc.) of the GSMA certificate to be issued, because they are anyways used to operate in a strict environment (well, at least theoretically).
I see the whole problem as a catch-22: we could definitely create an open-source SM-DP+, but what's the use if you cannot deploy to actual phones, only to your self-signed, custom eUICC. The main advantage of eSIM is lost as soon as you need to still use a plastic card. I'd rather explore the option of talking to the small SIM vendors that e.g. sysmocom uses and see if they would be open to run/get access to a production SM-DP+. Then we would have finally a solution to easily attach commercial phones to a custom network, e.g. at CCC with much less friction.

---

laforge #6 28 July 2023 09:21

> domi:
>
> I see the whole problem as a catch-22: we could definitely create an open-source SM-DP+, but what's the use if you cannot deploy to actual phones, only to your self-signed, custom eUICC. The main advantage of eSIM is lost as soon as you need to still use a plastic card.

You're thinking about this from a user point of view. I think about it from the developer / open source enthusiast point of view: What's the point investing time in something that doesn't result in open source software being created?

> domi:
>
> I'd rather explore the option of talking to the small SIM vendors that e.g. sysmocom uses and see if they would be open to run/get access to a production SM-DP+. Then we would have finally a solution to easily attach commercial phones to a custom network, e.g. at CCC with much less friction.

That might be an option technically and commercially (of course there will be cost associated with it, just like with physical cards). AFAICT, currently none of sysmocoms suppliers/business partners are active in the *consumer eSIM*, only in th *M2M* and possibly soon *IoT* eSIM (which have different architectures and are not interchangeable).

While I see the user benefit of it, I am rather hesitant to get sysmocom involved in something that doesn't really create open source software, or leads to any kind of "ownership". Conceptually, I am very much opposed to any kind of *as a service*. I believe in owning/controlling your own technology. Ideally with FOSS, but occasionally without it. What you are suggesting is just re-selling some service in which we'd have no power/control whatsoever. To me, that's ethically very questionable and I have an inherent repudiation towards that. I'm not saying we wouldn't ever do it if there really is a strong demand from customers and we find a partner to work with. Just explaining my thoughts.

1 Like

---

domi #7 28 July 2023 11:20

Yeah, I see your point. I also did not want to create the impression I want to push sysmocom towards this - first and foremost I have no authority to do so, and second of all I respect your philosophy behind it.
The only reason why I brought this up: the number 1 request I get from all around the telco community is that "I am able to run my own network, thanks to XYZ (OsmocomCNI, srsRAN, Open5GS, you name it), now how do I get people on it easily". Even this thread started with this question. Everybody wants to have commercial UEs out of the box attaching to their networks. Most, if not all private network usecases depend on this heavily as well.
Naturally it would be nice solving this, but the current solution to this is indeed subpar - especially if it involves, as you well said it depending on somebody's service and re-selling it.

---

laforge #8 20 October 2023 15:28

For the record, you may also find the recorded talk "demystifying esim technology" which I gave at CCC Camp 2023 (in August, after the original posting/discussion happened here) interesting: **media.ccc.de - Demystifying eSIM Technology**

2 Likes

---

tonisoft #9 22 October 2023 10:22

Thanks for the info, I'll check it out

---

mode51software #10 2 November 2023 23:56

> I see the whole problem as a catch-22: we could definitely create an open-source SM-DP+, but what's the use if you cannot deploy to actual phones, only to your self-signed, custom eUICC. The main advantage of eSIM is lost as soon as you need to still use a plastic card.

Having an eUICC in a physical SIM card form factor also has advantages if an end user wants to physically be able to remove it for security reasons. A key advantage over just a standard SIM is then being able to add and remove multiple profiles.

Comprion's 4FF test eUICC comes with an openly available test root specified in GSMA SGP.26 and Android does detect the additional eUICC. I note a custom app may be needed vs using the built in QR code scan, though this is possible with ARA-M carrier privileges.

For events like Chaos how about a model where an end user pre-purchases a sysmocom 4FF eUICC and then can reuse it at many events in the future. The user could grab an eSIM profile on arrival via an on-prem SM-DP+ with a matching root CA. None of the GSMA SAS requirements then apply.

I think there is merit in this in the same way as buying eg. a NeoPhone for the elevated security - specifically the comment in the Chaos talk about the external SM-DP+ provider having visibility of every EID that has downloaded a profile for the event.

If sysmocom were to provide this 4FF eUICC then an additional service could be to supply 4FF eUICCs with private roots and I think there would be value in doing this.

One other comment is that I found that the Pixel 6 has a second CA in the eUICC that I haven't been able to identify: **https://medium.com/p/154046762904**. Perhaps it is a Google test CA or a backup GSMA CA. It may be that some device manufacturers could provide devices with eUICCs in which a private root CA has been installed. Or provide a mechanism in which an additional private root CA could be dynamically added to an eUICC.

---

laforge #11 4 November 2023 10:21

> mode51software:
>
> Having an eUICC in a physical SIM card form factor also has advantages if an end user wants to physically be able to remove it for security reasons.

Yes. The main advantage also is that you can deploy eSIMs in devices that don't have eSIM support. Of course without an LPAd you cannot actually switch or download profiles, but you could remove the card, plug it into a card reader / your laptop and then do it there. Also, e.g. for cards permanentl installed in laptops one could run a LPAd speaking AT-commadnds for SIM card access (I believe this is what's happening in Chromebooks).

> mode51software:
>
> For events like Chaos how about a model where an end user pre-purchases a sysmocom 4FF eUICC and then can reuse it at many events in the future. The user could grab an eSIM profile on arrival via an on-prem SM-DP+ with a matching root CA. None of the GSMA SAS requirements then apply.

If the c3gsm team wanted that: Sourcing/Providing the eUICC with private CA root in 2FF/3FF/4FF seamless cut plastic card is no problem at all. The more interesting question is: Who will develop the "on-prem SM-DP+" and a LPAd (or test interop with existing LPAd in devices…).

> mode51software:
>
> If sysmocom were to provide this 4FF eUICC then an additional service could be to supply 4FF eUICCs with private roots and I think there would be value in doing this.

In fact at sysmocom we're planning to sell such cards (I have samples right in front of me), but the same problem applies: If there's not even a proof-of-concept that allows people in some way install/delete/activate/deactivate self-signed profiles on them, selling the eUICC will just create a support nightmare. And expecting that the profit on the few eUICC I expect us selling will cover the R&D of an (even only minimalistic) SM-DP+ is unrealistic…

> mode51software:
>
> One other comment is that I found that the Pixel 6 has a second CA in the eUICC that I haven't been able to identify: **https://medium.com/p/154046762904**. Perhaps it is a Google test CA or a backup GSMA CA. It may be that some device manufacturers could provide devices with eUICCs in which a private root CA has been installed. Or provide a mechanism in which an additional private root CA could be dynamically added to an eUICC.

I would find it extremely unlikely that it would be possible within the GSMA eSIM security profile to have additional, non-GSMA CA certificates present. Why would they permit that? There's nothing to be gained from it, and a lot to be lost if somehow that second root of trust could get access to any of the ISD-P and hence access critical data like key materials of an eSIM profile…

1 Like

---

mode51software #12 5 November 2023 12:13

> laforge:

> Yes. The main advantage also is that you can deploy eSIMs in devices that don't have eSIM support. Of course without an LPAd you cannot actually switch or download profiles, but you could remove the card, plug it into a card reader / your laptop and then do it there. Also, e.g. for cards permanentl installed in laptops one could run a LPAd speaking AT-commadnds for SIM card access (I believe this is what's happening in Chromebooks).

I think it's possible to use the built in Android LPA on eg. Pixel phones - Android auto detects the second eUICC in the physical SIM card. One issue is that the camera/QR code scanner uses the built in LPA, so a client carrier app will be required to control the flow. This would be ok though because having a client app is a substitute for a QR code and a better method. I plan to try and get a test app working (or not).

> laforge:
>
> If the c3gsm team wanted that: Sourcing/Providing the eUICC with private CA root in 2FF/3FF/4FF seamless cut plastic card is no problem at all. The more interesting question is: Who will develop the "on-prem SM-DP+" and a LPAd (or test interop with existing LPAd in devices…).

Awesome. I've been working on an SM-DP+ specifically for on-prem use cases. I've been using **Truphone's java LPA**. At this point I can create a SIM profile in a database and make requests using the Truhpone LPA (compiled from source) towards my locally hosted SM-DP+ and then it gets installed on the Comprion test eUICC via a USB SIM card reader. The whole webadmin piece/order management state machine backend isn't there yet and I'm thinking of a CLI for it as well (being able to create orders via pySim would be neat), but I need to prove that Android's LPA will work first. I've not decided on commercial models yet.

> laforge:
>
> In fact at sysmocom we're planning to sell such cards (I have samples right in front of me), but the same problem applies: If there's not even a proof-of-concept that allows people in some way install/delete/activate/deactivate self-signed profiles on them, selling the eUICC will just create a support nightmare. And expecting that the profit on the few eUICC I expect us selling will cover the R&D of an (even only minimalistic) SM-DP+ is unrealistic…

That's fantastic can you share any details on the version of SGP.22? Comprion's test eUICC is for v2.2.0. And also any constraints on the TCA profile version? Though using genericFileManagement I think I can add eg. 5G DFs even to a TCA v2.1 profile.

Infineon provides an online test SM-DP+ as well if the eUICC is Infineon based? I tried to get hold of an Infineon card with SGP.26 certs like the Comprion one but didn't get anywhere.

> laforge:
>
> I would find it extremely unlikely that it would be possible within the GSMA eSIM security profile to have additional, non-GSMA CA certificates present. Why would they permit that? There's nothing to be gained from it, and a lot to be lost if somehow that second root of trust could get access to any of the ISD-P and hence access critical data like key materials of an eSIM profile…

Fair point though then what is the other root? As Pixel devices come with an international ROM perhaps it is for eg. China, or perhaps it is a backup in case the main GSMA root is compromised. That's a point for the

comment on updateable roots - if the GSMA root is compromised then how can the roots be updated on existing devices? I suspect that the firmware in the eUICC can be updated and within that firmnware update the roots could also be updated. If that requires a visit to a service centre clearly it doesn't scale well! So perhaps the second root relates to something like an eUICC firmware update. I note the eUICC does report it's currently installed firmware version in the **eUICCInfo2 data struct**.

1 Like

---

laforge #13 6 November 2023 17:44

> mode51software:
>
> That's fantastic can you share any details on the version of SGP.22?

Right now we're working with SGP.22 v2.3. More recent SGP.22 v2.5 might be available in Q1/24 and v3.0 in Q3/24, though I cannot guarantee those dates, and we'll certainly make sure to sell all of our existing/old stock before ordering production runs with more up-to-date OS versions as they are available.

> mode51software:
>
> And also any constraints on the TCA profile version?

It is TCA eUICC profile package interop format V2.3.1

---

mode51software #14 6 November 2023 23:44

> laforge:
>
> Right now we're working with SGP.22 v2.3. More recent SGP.22 v2.5 might be available in Q1/24 and v3.0 in Q3/24, though I cannot guarantee those dates, and we'll certainly make sure to sell all of our existing/old stock before ordering production runs with more up-to-date OS versions as they are available.

Ok great will these appear on the sysmocom webshop or are they by request only? And perhaps only when more functionality has been added to pySim and there is a viable plan to provide SM-DP+ support?

Are there any SGP.31 cards? Being able to support SGP.31 in the same SM-DP+ codebase will clearly add extra value.

Another really major thing I'm looking out for is the Secured Applications for Mobile piece though it isn't clear what the delivery mechanism will look like yet other than that **"User Installs Service Provider App"**.

> laforge:

> It is TCA eUICC profile package interop format V2.3.1

Thanks ok.

---

laforge #15 7 November 2023 17:08

> mode51software:
>
> Ok great will these appear on the sysmocom webshop or are they by request only?

They will likely end up in the webshop (and a related news item on the website) once we are complete with testing/evaluating samples and order a first production batch.

> mode51software:
>
> Are there any SGP.31 cards?

I do not think any vendor is offering those yet, not even as engineering samples at this point. It's too early. AFAICT, there's not even a conformance test spec for SGP.32 yet, so nobody can verify a product even if they had one…

mode51software #16 8 November 2023 00:33

> laforge:
>
> They will likely end up in the webshop (and a related news item on the website) once we are complete with testing/evaluating samples and order a first production batch.

That's fantastic I'm really looking forward to that. I'll email about the SM-DP+ and post about the Android LPA control carrier app.

> laforge:
>
> I do not think any vendor is offering those yet, not even as engineering samples at this point. It's too early. AFAICT, there's not even a conformance test spec for SGP.32 yet, so nobody can verify a product even if they had one…

Sure - I think GSMA should provide an open source eUICC as a ref to use for integration testing for all these new specs.