iSIM ger liv till din IoT-vision

Av Simon Glassman och Samuele Falcomer, u-Blox

Simon Glassman är baserad i Storbritannien och har ansvar för att utveckla och genomföra strategiska samarbeten och partnerskapsprojekt. Fokus ligger framförallt på IoT över mobilnätet. Innan han började på u-Blox arbetade han på Numerex och TomTom.

Samuele Falcomer är produktlinjechef för IoT-produkter. Innan han började på u-Blox arbetade han med antenner och rf-teknik på Adanat och på Calearo Group.

IoT-utrustning på avlägsna platser använder typiskt mobilnätet både för att hämta in data och ta emot instruktioner. Det innebär att varje nod behöver ett SIM-kort (subscriber identity module) eller, som de kallades i äldre GSM- och UMTS-nät, ett UICC (universal integrated circuit card).

Det är i SIM-kortets integrerade krets som användaren identifieras och som krypteringsalgoritmerna lagras. Det ger åtkomst till mobilnätet, för som vi alla vet från våra mobiltelefoner – utan SIM-kort ingen tillgång till nätet (annat än för nödsamtal).

Det har skrivits mycket om de snabba framstegen inom IoT och om mobilnäten. Vad som inte har fått lika mycket uppmärksamhet är den samtidiga utvecklingen av SIM-tekniken. Den här artikeln syftar till att belysa den senaste versionen av SIM-kortet: iSIM, och varför det är en god nyhet för alla som utvecklar, bygger och driver mobila IoT-lösningar.

Men först lite historia för att ge en bakgrund och förstå de olika tekniker och akronymer som är relevanta för iSIM.

Det krympande SIM-kortet

Ett SIM-kort är en integrera krets som kör ett litet specialiserat operativsystem, SIM OS, och lagrar en unik identitet (IMSI, International Mobile Subscriber Identity) liksom uppgifter om operatören (MNO, Mobile Network Operator). Det gör det möjligt för abonnenten att ansluta till mobilnätet. MNO-profilen är programmerad i SIM-kortet på ett säkert sätt och innehåller nätverksåtkomstapplikationer, nycklar och autentiseringsuppgifter för en specifik nätverksoperatör.

Från att ha varit stora som kreditkort har SIM-korten gradvis krympt till miniformat, mikroformat och sedan nanoformat. Det som dock förblivit konstant är kravet på ett fysiskt element för att få tillgång till mobilnätet.

Framväxten av eSIM och eUICC

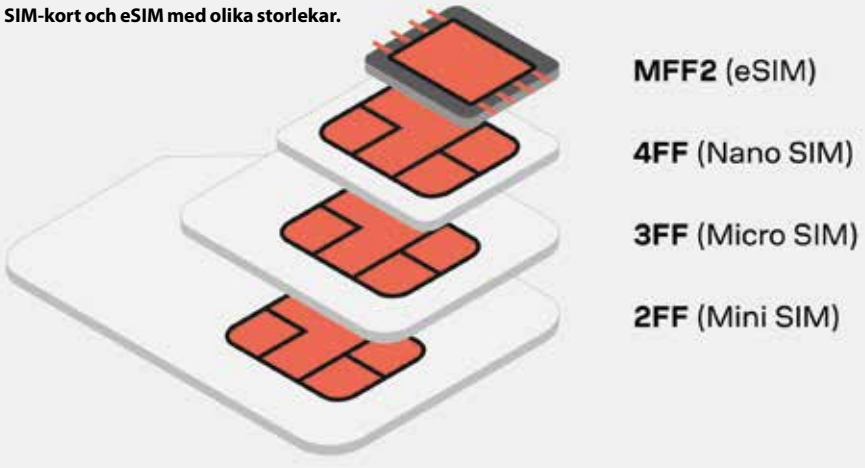
I början av 2010-talet dök det upp ett nytt alternativ: det inbäddade SIM-kortet, eller eSIM, som vanligtvis har formfaktorn MFF2. Det är ett SIM-chip som innehåller MNO-profilen och är fastlött på kretskortet. Jämfört med konventionella SIM-kort i plast är eSIM mindre, mer robusta, mer tillförlitliga och svårare att stjäla. Dessa egenskaper har gjort att eSIM har fått stort genomslag på marknaderna för fordon, olika typer av mätare och för industriell övervakning.

Vissa eSIM måste förladdas med en specifik MNO-profil medan andra kan laddas trådlöst (OTA) med hjälp av ett säkert RSP-system (remote SIM provisioning). Ett eSIM med denna OTA-förmåga kategoriseras som en eUICC. En eUICC är ett SIM-kort i valfri formfaktor som kan hantera trådlösa uppdateringarar av MNO-profilen.

Denna distinktion mellan eSIM och eUICC är viktig: termerna används ofta felaktigt som utbytbara. Detta kan leda till problem för den som tillverkar produkten och för operatörer när de upptäcker att de inte kan utföra en OTA-ändring av MNO-profilen på enheter som redan är ute i fält eftersom det eSIM de valt inte inkluderar eUICC-kapacitet eller har ett RSP-system.

I takt med att eUICC:er blev allt populärare utvecklades ett stort antal RSP-system för att hantera dem. Vissa var anpassade implementeringar, medan andra använde GSMA-standarder. Vi återkommer till det.

SIM-kort och eSIM med olika storlekar.



Misslyckade försök att eliminera det fysiska SIM-kortet

Efter att ha krympt SIM-kortet till minimal storlek gjordes försök att helt avveckla den fysiska enheten för att istället integrera allt i mobilens programvara. Dessa försök med ”mjuka SIM-kort” misslyckades av säkerhets- och integritetsskäl. En IoT-modul är inte tillräckligt säkrad för att kunna lagra ett SIM-operativsystem, inte ens med en så kallad ”trusted zone” i halvledarkretsen.

Därför vägrade de flesta mobiloperatörer att stödja mjuka SIM-kort. De få implementeringar som gjordes var anpassade SIM-kort som skapats i samarbete med en specifik mobiloperatör eller virtuell mobil-

”Uttrycket banbrytande används ofta, men i det här fallet tycker vi att det är passande”

operatör. Detta är slutna ekosystem och lösningen har inte varit särskilt framgångsrik.

Nästa iteration: iSIM

iSIM är nästa generation av SIM-kortet och medför den avveckling av hårdvaran som var tanken med mjuka SIM-kort. iSIM är en systemkrets med integrerade säkerhetsfunktioner i kislet (iSE, integrated secure element). Denna del är avskild från resten av kretsen och innehåller SIM OS och MNO-profilen. Det ger samma säkerhetsnivå och skydd mot manipulering som ett klassiskt SIM-kort eller eSIM.

iSIM kommer att medföra ett antal fördelar för dem som designar, tillverkar och använder IoT-enheter.

Bättre än SIM-kort i plast

Jämfört med konventionella SIM-kort i plast kräver iSIM mindre utrymme på kretskortet eftersom det inte behövs en SIM-hållare med tillhörande komponenter. iSIM är också mindre känsliga för vibrationer och temperaturväxlingar.

Dessutom förenklar de logistik, inköp och lagerhållning. Detta eftersom du inte behöver köpa SIM-korten i förväg, hantera lager av SIM-kort eller fysiskt sätta in SIM-kort i enheter inför leveransen. Du kan också lagerhålla färdiga IoT-enheter utan att behöva ha olika modeller för olika inbyggda SIM-kort. Istället kan man ha en enda modell och applicera en nätverksprofil på iSIM-kortet senare.

För de som distribuerar och använder IoT-enheter erbjuder iSIM också fördelar. En enhet med en eUICC iSIM och tillgång till ett RSP-system (mer om dessa nedan) kan använda olika MNO:er under sin livstid för att exempelvis dra nytta av billigare abonnemang när dessa blir tillgängliga. I länder där permanent roaming inte är möjligt kan enheterna enkelt kopplas till ett lokalt nätverk. Och allt detta kan göras utan att man fysiskt behöver byta SIM-kort, vilket skulle vara omöjligt i förseglade enheter, och dessutom dyrt och mycket komplext i allt annat än mycket små driftsättningar.

Sammantaget bidrar det till att sänka kostnaderna, förenkla driften och erbjuda verklig flexibilitet under hela livscykeln för IoT-enheten.

Fördelar relativt eSIM

Fördelarna med en iSIM jämfört med en eSIM är mindre men fortfarande betydande. Den viktigaste är att iSIM är ett SIM OS som körs på säker hårdvara i mobilens systemkrets medan ett eSIM är en säker krets som kör SIM OS och är fastlödd på kretskortet.

eSIM är en separat hårdvarukomponent som du måste köpa, profilera (om den inte har eUICC-kapacitet och du har ett RSP-system tillgängligt) och löda fast på ditt kort, utöver kommunikationsmodulen. Detta medför icke försumbara kostnader i samband med upphandling, tillverkning och logistik. Dessutom är eSIM vanligtvis förknippade med en minsta orderkvantitet som en IoT-enhet kanske inte (till en början) kan eller vill uppfylla.

En ny RSP-standard

För att iSIM ska få ett stort genomslag inom IoT-området krävs både eUICC-kapacitet och ett stödjande RSP-system som är anpassat till behoven hos enheter med begränsad nätverkskapacitet och användargränssnitt.

Fjärrstyrd SIM-tilldelning är redan vanligt i nya mobiler. Istället för att behöva sätta i ett fysiskt SIM-kort skannar konsumenterna en QR-kod med telefonens kamera. Detta aktiverar RSP-systemet och triggar nedladdningen av den relevanta MNO-profilen till enhetens eSIM. Processen fungerar på samma sätt med ett iSIM, den enda skillnaden är den fysiska plats där MNO-profilen lagras.

Varför har fjärrstyrd SIM-tilldelning inte fått så stor spridning inom mobiluppkopplade IoT-tillämpningar med tanke på hur smidig den är?

Det finns för närvarande två GSMA-kompatibla RSP-lösningar, inklusive en som är specifikt inriktad på maskin-till-maskin-miljöer (M2M) (GSMA SGP.01/.02). Båda är dock relativt datatunga och lämpar sig därför i allmänhet inte för IoT-enheter med begränsad energibudget som behöver minimera dataanvändningen.

Dessutom kräver standarden för M2M RSP GSMA att MNO pushar profilen till enheten. Det är inte IoT-enheten eller dess användare som initierar och äger kontrollen över RSP-processen, vilket begränsar flexibiliteten.

För att åtgärda detta arbetar GSMA med en ny standard som är särskilt utformad för IoT-enheter: SGP.31/.32. Den kommer att lanseras under första halvåret 2024 och kommer att vara avgörande för att möjliggöra ett brett införande av iSIM i IoT-enheter.

Spännande för tillverkare och operatörer

Vi är naturligtvis otroligt glada över de möjligheter som den här nya standarden kommer att öppna för alla dem som tillverkar och använder IoT-enheter. Uttrycket banbrytande används ofta, men i det här fallet tycker vi att det är passande. Det finns en chans att sänka både tillverknings- och driftskostnader, det finns en flexibilitet att med större lätthet kunna distribuera var som helst i världen och det finns en möjlighet att växla mellan olika MNO:er när så önskas. Med tanke på allt detta ser vi verkligen fram emot att få se vilka nya produkter och tjänster våra kunder kommer att ta till marknaden.

u-Blox välkomnar den gemensamma IoT RSP-standarden som utvecklas av GSMA. Och vi fortsätter att underhålla och utveckla en bred portfölj av cellulära IoT-moduler med traditionella formfaktorer – inklusive en nyligen lanserad modul med eSIM (SARA-R500E) för den nordamerikanska marknaden. ■