دوفصل‌نامه علمی منادی امنیت فضای تولید و تبادل اطلاعات (افتا)
سال ۱۴۰۵، جلد ۲۳، شماره ۲ (۱۲۵–۱۳۰)
https://monadi.isc.org.ir

ارائه‌شده در بیست و دومین کنفرانس بین‌المللی انجمن رمز ایران در دانشگاه شهید بهشتی، ۱۶ و ۱۷ مهرماه ۱۴۰۴

طراحی و توسعه سامانه یکپارچه مدیریت کلیدهای امنیتی اپراتور تلفن همراه (سیم‌کات)★

امیرحسین پورشمس* و علی احمدی بنی
شرکت ارتباطات سیار ایران، تهران، ایران

اطلاعات مقاله
کلمات کلیدی:
سیم‌کارت
کلید امنیتی
رمزنگاری
اپراتور
تلفن همراه
نوع مقاله: پژوهشی

چکیده

مدیریت امن کلیدهای رمزنگاری سیم‌کارت در اپراتورهای تلفن همراه، به‌ویژه در چرخه عمر کلیدها شامل تولید، ذخیره‌سازی، توزیع و بهره‌برداری، از چالش‌های اصلی امنیت سایبری به شمار می‌رود. این مقاله به بررسی موانع موجود در مدیریت کلیدهای سیم‌کارت در اپراتورهای تلفن همراه می‌پردازد و مسائلی نظیر تولید و انتقال غیرامن کلیدها، ذخیره‌سازی ناامن، نبود زیرساخت یکپارچه برای ارتباط با سامانه‌های مرتبط، فقدان سوابق جامع و متمرکز و ریسک تبانی یا سوءاستفاده را مورد توجه قرار می‌دهد. برای رفع این مشکلات، سامانه یکپارچه مدیریت کلیدهای امنیتی اپراتور تلفن همراه (سیم‌کات) طراحی و پیاده‌سازی شده است. این سامانه با بهره‌گیری از افزاره‌های امنیتی سخت‌افزاری بومی، الگوریتم‌های رمزنگاری پیشرفته و روش‌های تسهیم راز، امکان تولید، نگهداری و انتقال امن کلیدهای سیم‌کارت را فراهم می‌کند. همچنین با ارائه قابلیت‌هایی مانند احراز هویت دو عاملی، مدیریت متمرکز سوابق و پشتیبانی از مهاجرت به پیمانکاران جدید بدون ایجاد محدودیت، امنیت و کارایی فرایندهای مرتبط با کلیدهای سیم‌کارت را به‌طور چشمگیری ارتقا داده است. این راهکار به‌عنوان یک نوآوری جامع، نیازهای امنیتی اپراتورهای تلفن همراه را به صورت مؤثر برآورده می‌سازد.

© ۱۴۰۵ انجمن رمز ایران

۱ مقدمه

امروزه رمزنگاری به‌عنوان مرسوم‌ترین روش برای تضمین امنیت اطلاعات و ارتباطات به شمار می‌رود و به صورت گسترده در کاربردهای مختلف مورد استفاده قرار می‌گیرد. مهم‌ترین چالش امنیتی در سامانه‌های رمزنگاری، مدیریت کلیدهای رمزنگاری است. به این معنی که امنیت تمامی فرایندهای مرتبط با چرخه عمر کلید شامل تولید، ذخیره‌سازی، توزیع، نابودسازی، پشتیبان‌گیری، بازیابی و نیز به‌کارگیری کلید در حین اجرای الگوریتم‌های رمزنگاری باید تضمین گردد.

مسئله مدیریت کلید در یک اپراتور تلفن همراه به طور خاص به مسئله مدیریت چرخه عمر کلیدهایی گفته می‌شود که یک نسخه از آن‌ها بر روی سیم‌کارت و یک نسخه دیگر در پایگاه داده‌های اصلی اپراتور یا سامانه‌های اصلی مرتبط با آن قرار می‌گیرند. وظیفه این کلیدها تضمین امنیت ارتباطات نسل‌های مختلف شبکه موبایل و یا تضمین امنیت انواع برنامه‌های کاربردی است که بر روی سیم‌کارت فعال و اجرا می‌شوند.

در حال حاضر روند تولید مجموعه کلیدهای مورداستفاده در سیم‌کارت‌ها در بسیاری از اپراتورهای خاورمیانه، شامل فرایندهایی به صورت تولید دستی، انتقال توسط عاملی انسانی و ذخیره‌سازی بدون رمزنگاری است. تضمین امنیت شبکه اپراتور نیازمند ایجاد بستر مناسب برای ایجاد، نگهداری و بهره‌برداری از کلیدهای رمزنگاری بدون دخالت عامل انسانی

★از کمیته علمی بیستمین کنفرانس بین‌المللی انجمن رمز ایران برای داوری این مقاله تشکر می‌شود.
*نویسنده مسئول.
آدرس‌های رایانامه: ah.pourshams@mci.ir (امیرحسین پورشمس)، a.ahmadibeni@mci.ir (علی احمدی بنی)
© ۱۴۰۵ تمامی حقوق متعلق به انجمن رمز ایران است.

است. میلیون‌ها سیم‌کارت در اپراتورها وجود دارد و هر کدام از این سیم‌کارت‌ها بیش از ۳۰ کلید اختصاصی دارند که باید به صورت امن نگهداری شده و همچنین قابلیت متمرکزسازی نگهداری و توزیع امن کلید در اپراتور نیز وجود داشته باشد. علاوه بر این در راهکارهای فعلی در صورت مهاجرت از یک پیمانکار یا اپراتور به یک پیمانکار یا اپراتور دیگر، قابلیت انتقال کلید به زیرساخت جدید وجود ندارد و بایستی تمامی کلیدها به صورت دستی و فاش به پیمانکار جدید تحویل گردد. وجود این چالش‌ها و محدودیت‌ها ضرورت توسعه راهکاری جامع و امن در مسئله مدیریت کلید را بیش از پیش نمایان می‌سازد.

۲ تعریف مشکل و چالش‌ها

کلیدهای سیم‌کارت‌ها به‌عنوان یکی از حیاتی‌ترین دارایی‌های هر اپراتوری محسوب می‌گردند و افشا شدن آنها تبعات سنگینی از بُعد امنیت خواهد داشت. لذا حفظ امنیت این کلیدها اهمیت ویژه‌ای در اپراتورها دارد. در ادامه مهم‌ترین چالش‌ها در طی فرایند تولید و مدیریت کلیدهای سیم‌کارت بیان می‌گردند.

۱.۲ تولید و انتقال امن کلید

علی‌رغم اهمیت کلیدهای سیم‌کارت، اکثر اپراتورهای خاورمیانه فرایند امنی جهت تولید و مدیریت چرخه عمر این کلیدها ندارند و در طی فرایند تولید و مدیریت کلیدهای سیم‌کارت نقش عامل انسانی بسیار پررنگ بوده و عموما از استانداردهای تولید کلید رمزنگاری استفاده نمی‌شود و از مرحله تولید کلید تا انتقال کلید به مولفه‌های مختلف اپراتور امکان فاش شدن کلیدهای مختلف سیم‌کارت وجود دارد مثلاً ممکن است کلیدها بر روی رسانه‌های ناامن (یک تکه کاغذ، یک فایل بر روی یک حافظه فلش یا یک لپ‌تاپ) قرار گیرند. در نتیجه امکان فاش شدن این کلیدها یا به سرقت رفتن آن وجود دارد.

۲.۲ نگهداری امن کلید

پس از تولید کلیدهای سیم‌کارت که هر کدام دارای یک بر چسب دوبیتی هستند و نوع آن را مشخص می‌کند، نگهداری آنها به صورت امن چالش بعدی اپراتورها است. به نحوی که سطح امنیتی هر کلیدی که نگهداری می‌شود، وابسته به برخی صفات امنیتی آن کلید است. دراین‌رابطه و به طور خاص، سه صفت امنیتی زیر اهمیت دارند:

- محرمانه بودن [1]: اگر صفت محرمانه برای یک کلید مقداردهی شده باشد، استفاده عملیاتی از آن کلید (رمزگذاری/رمزگشایی با استفاده از آن کلید) تنها زمانی مجاز است که کاربر یا برنامه کاربردی مجاز شده باشد.
- حساس [2]: اگر صفت حساس برای یک کلید مقداردهی شده باشد، هرگز نباید به صورت غیررمزشده امکان استخراج آن کلید وجود داشته باشد و باید فقط به صورت رمزشده استخراج گردد.
- غیرقابل استخراج [3]: اگر این صفت برای یک کلید مقداردهی شده باشد، استخراج کلید حتی به صورت رمزشده امکان‌پذیر نیست. یعنی هیچ راهی برای خارج کردن کلید یا دسترسی به محتوای فاش آن به صورت یکپارچه وجود ندارد.

۳.۲ ارتباط با سایر سامانه‌ها

علاوه بر اینکه نگهداری امن کلیدهای سیم‌کارت مهم است دسترسی پذیری توسط سایر سامانه‌های مرتبط و انتقال امن به آنها نیز ضرورت دارد و در این مرحله اپراتورها با چالش‌های مختلفی مواجه هستند. به منظور مبادله کلید میان دو مؤلفه به صورت خودکار و بدون دخالت عامل انسانی، لازم است دو مؤلفه با استفاده از واسط استانداردی که توسط هر دو مؤلفه پشتیبانی می‌گردد با یکدیگر تعامل داشته باشند که در پیاده سازی‌های فعلی چنین شرایطی فراهم نیست.

۴.۲ نگهداری سوابق سیم‌کارت‌ها

اپراتورها نیازمند بستری جامع برای دسترسی کامل به سوابق سیم‌کارت و کلیدهای آن هستند که علاوه بر نگهداری کلیدهای سیم‌کارت سوابق مربوط به هر سیم‌کارت حتی سیم‌کارت‌هایی که غیرفعال شده‌اند را نیز دارا باشد. با توجه به حجم بالای اطلاعات نیاز به استفاده از بسترهای پردازشی کلان داده وجود دارد که این امکان در اپراتورها به صورت یک سامانه جامع وجود ندارد و باید به صورت دستی بین داده‌های چند سامانه همبسته‌سازی ایجاد شود که بازهم تمام خواسته‌ها را مرتفع نمی‌سازد و ممکن است داده‌ها ناقص بوده یا به خروجی مطلوب منتج نشوند.

۵.۲ جلوگیری از تبانی و سوء استفاده

با توجه به دخیل بودن عامل انسانی در تولید و مدیریت کلیدهای انتقال، یکی دیگر از مشکلات امکان تبانی افراد در جهت افشاء اطلاعات است که می‌تواند ابعاد مختلفی را در بر داشته باشد، لذا باید به نحوی باشد که با تبانی افراد دخیل در یک بخش امکان افشاء و سوءاستفاده از کلیدهای انتقال در راستای دستیابی به کلیدهای سیم‌کارت وجود نداشته باشد و استفاده از کلید انتقال تنها با استفاده از الگوریتم‌های تسهیم راز نظیر شامیر [۱] ممکن باشد.

۶.۲ امکان تعریف و مهاجرت به هر پیمانکار جدید

از دیگر نیازمندی‌های اپراتورها امکان مهاجرت از یک پیمانکار به یک پیمانکار دیگر است. مثلاً اگر به هر دلیلی لازم باشد شرکت نوکیا جایگزین شرکت هوآوی گردد در چنین شرایطی با در نظر گرفتن اینکه میلیون‌ها سیم‌کارت در شبکه فعال هستند، نباید این جایگزینی باعث از دست رفتن اطلاعات و کلیدهای سیم‌کارت‌های قدیمی گردد [۲]. به عبارت

[1] Private [2] Sensitive

[3] UnExtractable

دیگر مشترکان قبلی با همان سیم‌کارت‌های قدیمی باید بتوانند از امکانات فراهم شده توسط سامانه‌های جدید استفاده کنند.

۳ ارائه تجربیات و دستاوردها

به منظور برآورده کردن نیازمندی‌های امنیتی و عملکردی اپراتورهای تلفن همراه در رابطه با مسئله مدیریت کلیدهای سیم‌کارت‌ها، پروژه «طراحی و توسعه سامانه یکپارچه مدیریت کلیدهای امنیتی اپراتور تلفن همراه» اجرا شد. هدف این پروژه تضمین کیفیت چرخه تولید، نگهداری و بهره‌برداری کلیدهای رمزنگاری مورد استفاده در سیم‌کارت‌ها است. این هدف با اتکای به تعدادی افزاره امنیتی سخت‌افزاری [1] بومی و سامانه یکپارچه مدیریت کلیدهای امنیتی اپراتور تلفن همراه (سیم‌کات) انجام می‌گیرد. سامانه سیم‌کات مسؤول دریافت کلیدهای سیم‌کارت از پیمانکاران شخصی‌سازی سیم‌کارت، نگهداری کلیدهای سیم‌کارت و کلیدهای انتقال در یک پایگاه داده متمرکز و توزیع کلیدهای سیم‌کارت مورد نیاز در سامانه‌های مختلف اپراتور از جمله پایگاه داده مشترکین است. در ادامه مراحل رفع چالش‌های مختلف و نیز نوآوری‌های صورت گرفته تشریح می‌گردد.

۱.۳ انواع کلید و کاربرد آنها

در طی چرخه تولید کلیدهای سیم‌کارت تعدادی کلید دیگر نیز مورد استفاده قرار می‌گیرند از جمله:

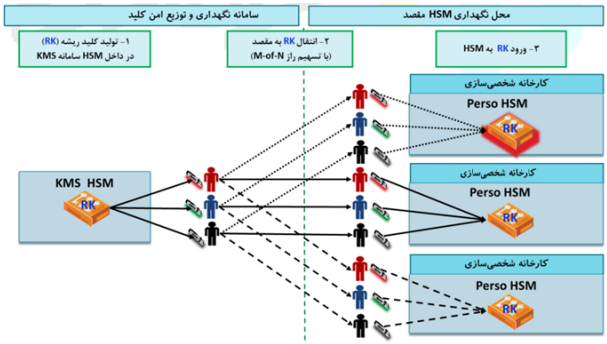
- کلید انتقال: برای رمز کردن کلیدهای اصلی سیم‌کارت هنگام انتقال بین مؤلفه‌های مختلف اپراتور استفاده می‌شود.
- کلید ریشه: کلیدی که میان، افزاره‌های امنیتی سخت‌افزاری در بخش‌های مختلف سامانه برای انتقال رمزشده کلیدهای سیم‌کارت استفاده می‌شود.

۲.۳ استقرار و همگام سازی افزاره‌های امنیتی سخت‌افزاری

در اولین گام برای برآورده کردن نیازها و رفع چالش‌های تولید و نگهداری امن کلیدهای تولید شده، یک دستگاه افزاره امنیتی سخت‌افزاری در کنار سامانه سیم‌کات قرار گرفته و به هرکدام از کارخانه‌های تولید سیم‌کارت نیز یک افزاره امنیتی سخت‌افزاری داده می‌شود، از این افزاره امنیتی سخت‌افزاری برای تولید کلید انتقال و نیز نگهداری کلیدهای سیم‌کارت استفاده خواهد شدکه مراحل آن به شرح زیر است.

۳.۳ تولید و انتشار امن کلید ریشه در افزاره امنیتی سخت‌افزاری

در فرایند مدیریت کلید، ابتدا کلید ریشه در افزاره امنیتی سخت‌افزاری متصل به سامانه سیم‌کات تولید و سپس بین سایر افزاره امنیتی سخت‌افزاری اشتراک گذاری می‌شود. شکل ۱ مبادله کلید ریشه بین افزاره‌های امنیتی سخت‌افزاری در طرح انتقال کلید را نشان می‌دهد. در



شکل ۱. مبادله کلید ریشه بین افزاره‌های امنیتی سخت‌افزاری

خصوص ایجاد کلید ریشه و مبادله آن نکات زیر مدنظر است:

- کلید ریشه در افزاره امنیتی سخت‌افزاری متصل به سامانه سیم‌کات تولید می‌شود.
- مبادله کلید ریشه بین افزاره امنیتی سخت‌افزاری متصل به سامانه سیم‌کات و سایر افزاره‌های امنیتی سخت‌افزاری به صورت آفلاین و مبتنی بر تسهیم راز M-of-N با استفاده از توکن‌های USB صورت می‌گیرد.

تولید و مبادله کلید ریشه معمولاً فقط با یک بار اجرا در طول عمر سامانه صورت می‌گیرد. پس از مبادله کلید بین افزاره‌های امنیتی سخت‌افزاری، می‌توان اقدام به انتقال امن کلیدهای سیم کارت به صورت رمزشده با کلید ریشه نمود. بر اساس طرح تسهیم راز M-of-N هیچ کدام از این N نفر به تنهایی نمی‌توانند از محتوای کلید ریشه مطلع گردند. فقط زمانی که حداقل M نفر از این N نفر حضور داشته باشند، از نظر ریاضی امکان بازیابی کلید ریشه وجود دارد. همچنین با توجه به اینکه هر کدام از توکن‌های USB با گذرواژه یکتایی که تنها در اختیار فرد نگهدارنده توکن است محافظت می‌شوند، در صورت به سرقت رفتن توکن‌ها نیز خطری امنیت کلید ریشه را تهدید نمی‌کند.

۴.۳ فرآیند تولید و مبادله کلید انتقال

سامانه سیم‌کات با اتصال به افزاره امنیتی سخت‌افزاری اختصاصی خود دستور تولید کلید انتقال را صادر نموده و کلیدهای انتقال تولید و درون افزاره امنیتی سخت‌افزاری ذخیره می‌گردند. این کلیدها برای انتقال کلیدهای سیم‌کارت تولید شده در کارخانه‌های شخصی‌سازی استفاده می‌گردد. کلیدهای انتقال به وسیله کلید ریشه افزاره امنیتی سخت‌افزاری رمزگذاری شده و با استفاده از الگوریتم تسهیم راز کلیدها به افزاره امنیتی سخت‌افزاری کارخانه منتقل می‌گردند. در افزاره امنیتی سخت‌افزاری برای تولید کلیدهای رمزنگاری از مولد سخت‌افزاری عدد تصادفی واقعی استفاده می‌شود که با استانداردسطح سوم FIPS 140-2 سازگار است و امنیت بالایی را تضمین می‌کند. برای رمزگذاری، الگوریتم‌های استاندارد مانند AES-256، RSA و ECC به کار می‌روند که با استفاده PKCS#11 مدیریت می‌شوند. این رویکرد، امنیت و یکپارچگی داده‌ها را در برابر تهدیدات پیشرفته تضمین می‌کند.

[1] Hardware Security Module (HSM)

۵.۳ نگهداری امن کلید و انتقال به سایر سامانه‌ها

کلیدهای سیم‌کارت‌ها با استفاده از کلید انتقال رمزشده و به افزاره امنیتی سخت‌افزاری سامانه سیم‌کات منتقل می‌شوند. از این پس این کلیدها به صورت رمزشده و ایمن در سامانه نگهداری می‌شوند و برای انتقال کلید هر سیم‌کارت نیاز به اجرای فرایندی جهت تایید انتقال آن کلید است. طی این فرایند تمام واحدهای ذی‌ربط باید این درخواست را تایید کنند تا فرایند انتقال کلید انجام پذیرد و گزارش مربوط به این انتقال در سامانه‌ها به صورت غیر قابل ویرایش ذخیره گردد.

از دیگر نوآوری‌های اصلی این محصول رفع محدودیت انتقال کلید به مؤلفه‌های دیگر نظیر افزاره امنیتی سخت‌افزاری سایر تولیدکنندگان و نیز سایر سامانه‌های مدیریت کلید است، تحت این راهکار، تمام کلیدهای سیم‌کارت به صورت کاملاً امن و رمزشده قابلیت انتقال به سامانه‌های مورد نظر را دارند.

۶.۳ سامانه جامع مدیریت کلید

از اصلی‌ترین نیازمندی‌های اپراتورها، مدیریت کلیدهای سیم‌کارت و سوابق مربوط به آن‌ها است، به نحوی که تمام رخدادها و عملیات‌های مرتبط با کلیدهای هر سیم‌کارت قابل دستیابی بوده و نیز بتوان با سرعت در آنها جست و جو کرده و گزارش دریافت کرد [۳]. در این سامانه با پیاده سازی شاخص گذاری اطلاعات به فرآیند جست و جو سرعت بخشیده شده است.

۷.۳ کارکردهای امنیتی سامانه

۱.۷.۳ احراز اصالت مبتنی بر توکن USB

برای سامانه‌هایی که سطح امنیت بالاتری نیاز دارند، از فرایندهای احراز اصالت دو عاملی مانند احراز اصالت مبتنی بر توکن استفاده می‌شود. یعنی کاربران علاوه بر دانستن یک گذرواژه، نیازمند یک عامل دیگر برای احزار اصالت هستند. این عامل می‌تواند یک توکن USB باشد که برای کاربران مجاز تعریف شده و در اختیار آنها قرار می‌گیرد و در زمان احراز اصالت باید به سیستم کاربر متصل باشد. سامانه سیم‌کات این نوع احراز اصالت را نیز پشتیبانی می‌کند. انتخاب روش احراز اصالت (مبتنی بر گذرواژه یا مبتنی بر توکن) توسط راهبر سامانه در تنظیمات امنیتی آن قابل انتخاب است.

۲.۷.۳ احراز اصالت کاربران افزاره امنیتی سخت‌افزاری

افزاره‌های امنیتی سخت‌افزاری مورد استفاده در سامانه سیم‌کات سطح سوم از استاندارد FIPS 140-2 پیکربندی می‌شوند. در نتیجه تصدیق اصالت کاربران این افزاره امنیتی سخت‌افزاری با استفاده از توکن‌های USB و به صورت دوعاملی انجام می‌گیرد. احراز اصالت باید به صورت تسهیم راز M از N باشد. بدین معنی که در زمان راه اندازی افزاره امنیتی سخت‌افزاری توکن‌های مورد نظر، تعریف و به کاربران تخصیص داده می‌شوند. سپس در صورت پیکربندی افزاره امنیتی سخت‌افزاری به صورت M از N انجام هر گونه عملیات روی افزاره امنیتی سخت‌افزاری مانند تولید یا انتقال کلید نیازمند لاگین به پارتیشن مورد نظر با حضور حداقل M نماینده از N نماینده که توکن را در اختیار دارند است.

۴ نتیجه‌گیری

از بزرگ‌ترین چالش‌های امنیتی اپراتورهای تلفن همراه امنیت کلیدهای سیم‌کارت است. به نحوی که علاوه بر حفظ محرمانگی کلیدها امکان استفاده از آنها در سایر سامانه‌های اپراتور وجود داشته باشد. در این راهکار با معرفی سامانه سیم‌کات که به بهره‌گیری از ماژول امنیت سخت‌افزاری اختصاصی‌سازی شده در کنار توسعه نرم افزار اختصاصی می‌پردازد، چالش‌های موجود از جمله نحوه تولید کلید، ذخیره‌سازی امن کلیدها و جلوگیری از تبانی افراد برای افشا کلید مرتفع گردیدند. همچنین سعی شد پیاده سازی محصول به نحوی باشد که با ارائه راهکار انتقال امن محدودیت‌های مرتبط با پیمانکار و محصولات هم تا حد امکان رفع گردد و در صورت تغییر پیمانکار در اپراتورها محدودیتی در خصوص کارکرد سامانه‌ها و نیز سیم‌کارت‌های قدیمی وجود نداشته باشد. در نهایت سامانه سیم‌کات به عنوان راهکاری نوآورانه در جهت رفع نیازهای امنیتی اپراتورهای تلفن همراه به بهره برداری رسید.

۵ سپاس‌گزاری

از تمام همکاران شرکت ارتباطات سیار که در پیش‌برد این پروژه بزرگ و پیچیده همکاری نموده اند کمال تشکر و قدردانی را داریم.

مراجع

[1] Shamir, Adi. How to share a secret. Communications of the ACM, 22(11):612–613, 1979.

[2] TECHNICAL SPECIFICATION, “ETSI TS 102 223 V14.0.0 (2017-05),” Etsi.org. [Online].

[3] TECHNICAL SPECIFICATION, “ETSI TS 131 111 V17.6.0 (2023-01),” Etsi.org. [Online].

MonadiAfta-Bianual Scientific Journal for Cyberspace Security
2026, Volume 23, Number 2 (pp. 125–130)
https://monadi.isc.org.ir

Presented at the ISCISC 2025 in Shahid Beheshti University, Tehran, Iran

Design and development of a secure and integrated cryptographic key management system for mobile network operators (SIMKAT)★

Amirhossein Pourshams * and Ali Ahmadi Beni

Mobile Communications Company of Iran (MCI), Iran

EXTENDED ABSTRACT

Keywords:
SIM card, Security key, Cryptography, Mobile network operator, Mobile phone

Type: Research paper

Cryptography is the foundation of modern information security and is extensively used to protect communications, digital services, and critical infrastructures. The effectiveness of any cryptographic system depends heavily on the secure management of cryptographic keys throughout their lifecycle. Key lifecycle management includes key generation, storage, distribution, usage, backup, recovery, and destruction. Any weakness in these processes can compromise the security of the entire system. In mobile network operators, SIM card cryptographic keys represent one of the most sensitive assets because they are responsible for subscriber authentication, secure communication, and the protection of SIM-based applications.

A copy of each SIM card key is stored within the SIM card, while another copy is maintained in the operator's core systems and subscriber databases. Consequently, protecting these keys is essential for ensuring network security. However, in many telecommunications environments, especially within developing regions, the management of SIM card keys still relies on manual procedures. Human involvement in key generation, transfer, and storage increases the risk of key exposure, insider threats, and operational errors. In some cases, keys may be temporarily stored on insecure media such as files, laptops, removable storage devices, or even printed documents, creating opportunities for unauthorized disclosure.

Beyond secure generation and transfer, operators face additional challenges related to key storage and access control. Different cryptographic keys require different levels of protection based on their security attributes. Confidential keys should only be accessible to authorized users or applications, sensitive keys should never be extracted in plaintext form, and non-extractable keys must remain protected inside secure cryptographic hardware. Managing these requirements for millions of SIM cards creates significant technical and operational complexity.

Another important challenge is the secure exchange of cryptographic keys between different systems. Existing infrastructures often lack standardized mechanisms for automated key distribution, forcing organizations to depend on manual processes and vendor-specific solutions. Furthermore, operators require comprehensive historical records associated with SIM cards and their keys for operational and auditing purposes. The large volume of data involved makes centralized management and rapid retrieval difficult without a dedicated platform.

Insider threats and collusion among personnel also represent a serious concern. Since multiple individuals may participate in key management operations, there must be mechanisms that prevent any single person—or even a small group—from gaining unauthorized access to critical cryptographic assets. In addition, operators often

★ The ISCISC 2025 Program Committee effort is highly acknowledged for reviewing this paper.
* Corresponding author
Email addresses: ah.pourshams@mci.ir (Amirhossein Pourshams), a.ahmadibeni@mci.ir (Ali Ahmadi Beni)
© 2026 ISC. All rights reserved.

encounter difficulties when migrating from one equipment vendor to another. Existing approaches frequently require the insecure transfer of cryptographic keys, increasing security risks and limiting operational flexibility.

To address these challenges, an integrated solution called SIMKAT was designed and developed. The objective of SIMKAT is to provide a secure and centralized infrastructure for the complete lifecycle management of SIM card cryptographic keys while minimizing human intervention and improving security throughout the key lifecycle.

The proposed solution combines dedicated Hardware Security Modules (HSMs) with a centralized software platform. SIMKAT is responsible for receiving SIM card keys from SIM personalization facilities, securely storing them, managing key-related operations, and distributing authorized keys to subscriber databases and other operator systems. By integrating hardware-based security with software-controlled workflows, the system provides comprehensive protection for cryptographic assets throughout their lifecycle.

The architecture employs multiple categories of keys, including SIM card keys, transport keys, and root keys. Root keys are generated within trusted HSM devices and are used to secure the encrypted transfer of SIM card keys between HSMs. To ensure maximum protection, root key distribution is performed offline using an M-of-N secret-sharing mechanism based on Shamir's Secret Sharing Scheme. Under this approach, no individual participant possesses sufficient information to reconstruct the root key independently. The key can only be recovered when a predefined minimum number of authorized participants collaborate. This mechanism significantly reduces the risks associated with insider threats and unauthorized disclosure.

Transport keys are generated and stored within HSM devices using hardware-based true random number generators compliant with FIPS 140-2 Level 3 security requirements. Standard cryptographic algorithms such as AES-256, RSA, and Elliptic Curve Cryptography (ECC) are employed to provide strong protection for key management operations. Key management functions are implemented through standardized interfaces, ensuring interoperability between different systems and vendors.

After generation, SIM card keys are encrypted using transport keys and securely transferred to the SIMKAT platform. The keys remain protected throughout their lifecycle and are only accessible through controlled and authorized processes. Any request for key transfer or operational use must pass through predefined approval workflows involving authorized personnel. All activities are recorded in immutable audit logs, ensuring accountability, traceability, and compliance with security policies.

One of the most important innovations of the proposed solution is its ability to securely exchange encrypted SIM card keys with systems developed by different vendors. Unlike traditional approaches that require exposing keys during migration processes, SIMKAT enables secure interoperability without compromising confidentiality. As a result, mobile network operators can replace infrastructure vendors while preserving existing subscriber information and cryptographic assets. This capability supports secure migration between vendors and eliminates the need to replace existing SIM cards during infrastructure upgrades.

The platform also incorporates advanced authentication and access-control mechanisms. For sensitive operations, two-factor authentication based on USB security tokens is supported. Furthermore, operations performed on HSM devices require multi-person authorization through M-of-N authentication policies. Critical operations involving cryptographic keys can only be executed when the required number of authorized representatives are simultaneously present and authenticated. These controls provide an additional layer of protection against insider misuse and unauthorized actions.

To support operational requirements, SIMKAT includes a centralized repository capable of maintaining complete historical records associated with SIM cards and their cryptographic keys. Efficient indexing and search mechanisms enable rapid retrieval of information even in environments containing millions of records. This functionality improves operational visibility and supports auditing and reporting activities.

In conclusion, SIM card cryptographic keys are among the most critical security assets of mobile network operators. Traditional key management approaches suffer from significant limitations, including manual processes, inadequate protection mechanisms, interoperability challenges, insider threats, and vendor dependency. The SIMKAT platform addresses these issues through the integration of hardware-based security, centralized lifecycle management, secure key distribution, secret-sharing mechanisms, and advanced authentication controls. The resulting solution provides a secure framework for managing SIM card cryptographic keys while supporting interoperability and secure migration between different vendors.