UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
Faculdade de Engenharia e Ciências de Guaratinguetá

BRUNO KENZO SUZUKI

Análise de cartões (U)SIM: universal integrated circuit card, comandos APDU, SIM toolkit e autenticação em redes 2G e 3G

Guaratinguetá

2023

BRUNO KENZO SUZUKI

Análise de cartões (U)SIM: universal integrated circuit card, comandos APDU, SIM toolkit e autenticação em redes 2G e 3G

Trabalho de Graduação apresentado ao Conselho de Curso de Graduação em Engenharia Elétrica da Faculdade de Engenharia e Ciências do Campus de Guaratinguetá, Universidade Estadual Paulista, como parte dos requisitos para obtenção do diploma de Graduação em Engenharia Elétrica.

Orientador (a): Prof. Dr. Daniel Julien Barros da Silva Sampaio

Guaratinguetá

2023

Suzuki, Bruno Kenzo
S264a Análise de cartões (U)SIM: universal integrated circuit card, comandos APDU, SIM toolkit e autenticação em redes 2G e 3G / Bruno Kenzo Suzuki - Guaratinguetá, 2023.
52 f : il.
Bibliografia: f. 46-47

Trabalho de Graduação em Engenharia Elétrica – Universidade Estadual Paulista, Faculdade de Engenharia e Ciências de Guaratinguetá, 2023.
Orientador: Prof. Dr. Daniel Julien B. da Silva Sampaio

1. Sistemas operacionais (Computadores).
2. Smartphones. 3. Armazenamento de dados.
4. Indústria de tecnologia de ponta.
I. Título.

CDU 681.3.062

Luciana Máximo
Bibliotecária/CRB-8 3595

UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
Faculdade de Engenharia e Ciências de Guaratinguetá

BRUNO KENZO SUZUKI

ESTE TRABALHO DE GRADUAÇÃO FOI JULGADO ADEQUADO COMO PARTE DO REQUISITO PARA A OBTENÇÃO DO DIPLOMA DE **"GRADUADO EM ENGENHARIA ELÉTRICA"**

APROVADO EM SUA FORMA FINAL PELO CONSELHO DE CURSO DE GRADUAÇÃO EM NOME DO CURSO

Prof. Dr. Daniel Julien Barros da Silva Sampaio
Coordenador

BANCA EXAMINADORA:

Prof. Dr. Daniel Julien Barros da Silva Sampaio
Orientador/UNESP-FEG

Prof. Dr. Samuel Euzédice de Lucena
UNESP-FEG

Prof. MSc. Thiago José Michelin
UNESP-FEG

Janeiro 2023

DADOS CURRICULARES

BRUNO KENZO SUZUKI

NASCIMENTO 03.05.1999 – Mogi das Cruzes / SP

FILIAÇÃO Edson Yuichi Suzuki
Luciene Chaves Muniz Suzuki

Dedico este trabalho à minha família e a todos que me acompanharam nesta jornada.

AGRADECIMENTOS

É quase impossível começar esses agradecimentos sem falar sobre os grandes responsáveis pela minha formação como ser humano. Sendo assim, em primeiro lugar, gostaria de agradecer aos meus pais, *Luciene Chaves Muniz Suzuki* e *Edson Yuichi Suzuki*, que sempre estiveram presentes oferecendo o melhor que podiam para o meu crescimento pessoal e profissional. Quando se trata de criação, também sou grato ao apoio e amor incondicional dos meus avós paternos, *Yasuko Suzuki* e *Mario Suzuki*, e da minha avó materna, *Luzia Chaves*. Ao meu irmão, *Nicolas Tadashi Suzuki*, minha gratidão por todos os anos de companheirismo desde a infância até a vida adulta;

ao meu orientador, *Prof. Dr. Daniel Julien Barros da Silva Sampaio*, que sempre esteve aberto para escutar as minhas ideias e se dispôs a me acompanhar e auxiliar na execução deste trabalho;

aos meus amigos da faculdade, *Bruno Hideki Yoshida*, *Fábio Augusto Abreu Gama dos Santos*, *Guilherme Cavalcante da Silva*, *Marcus Vinícius Simões* e *Rodrigo Carvalho Guerra*, agradeço o companheirismo que perdurou durante toda a faculdade. O apoio diário fez com que a amizade se fortalecesse para além da graduação;

à minha namorada *Beatriz Calais* e aos meus amigos de Mogi das Cruzes, *Julia Vilela, Alessandro Campos Mauro, Antonio Bruno Nonato, Gabriel Steidle Castrezano*, *Guilherme Stolemberger* e *Matheus Henrique Souza Campos*, sou grato por estarem presentes há tanto tempo na minha vida;

aos meus amigos *Eliezer Taffuri* e *Leonardo Amaro*, agradeço por todas as noites de videogame que me alegraram e me fizeram aliviar as ansiedades do dia a dia, além das conversas e conselhos;

à toda equipe TC LAS e eTC LATAM da Thales, empresa que me recebeu como estagiário e abriu as portas para a minha efetivação. Um agradecimento especial ao *Danilo Marquette Lima* por ter acreditado no meu potencial e pelos desafios e ensinamentos que me ajudaram a crescer profissionalmente.

RESUMO

Por meio do estudo das normas, este trabalho foi feito com a intenção de criar um material de apresentação sobre o universo dos cartões (U)SIM. A partir da introdução, explicação e retomada histórica sobre os conceitos básicos para o entendimento do assunto, foi possível se aprofundar em questões mais complexas, como a estrutura de arquivos e suas principais características e a autenticação em redes 2G e 3G. Além dos seis capítulos com as principais informações para quem busca começar a entender sobre o funcionamento dos cartões (U)SIM, também há dois apêndices com exemplos que ajudam na percepção prática de tópicos discutidos ao longo do trabalho. Em um deles, foi feito um programa em Phyton para envio de comandos APDU – o que complementa o conteúdo sobre suas características e funcionamento. De forma geral, o trabalho busca atuar como base informativa para aqueles que possuem interesse em se aprofundar na temática.

PALAVRAS-CHAVE: Smart Card; Cartão (U)SIM; Comandos APDU; SIM Toolkit; Autenticação.

ABSTRACT

This work was done with the intention of creating a presentation material about the universe of (U)SIM cards. Through the study of standards, the introduction, explanation, and historical review of the basic concepts for understanding the subject were covered. It was then possible to delve into more complex issues, such as the file structure, its main characteristics, and authentication in 2G and 3G networks. The work consists of six chapters containing the main information for those looking to begin to understand how (U)SIM cards work, and two appendices with examples that help in the practical perception of topics discussed throughout the work. In one of the appendices, a Phyton program was created to send APDU commands, which complements the content about its characteristics and functioning. In general, the work aims to act as an informative base for those interested in delving deeper into the subject.

KEYWORDS: Smart Card; (U)SIM Card; APDU Commands; SIM Toolkit; Authentication.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

APDU	Application Protocol Data Unit
AUTN	Authentication Token
AUTS	Re-synchronization Token
AuC	Authentication Center
CAT	Card Application Toolkit
ETSI	European Telecommunications Standards Institute
GSM	Global System for Mobile communications
HLR	Home Location Register
ICCID	Integrated Circuit Card Identification
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
ISIM	IMS Subscriber Identity Module
ITU	International Telecommunication Union
LTE	Long Term Evolution
ME	Mobile Equipment
NAA	Network Access Application
NR	New Radio
SIM	Subscriber Identity Module
STK	SIM Toolkit
USIM	Universal Subscriber Identity Module
UICC	Universal Integrated Circuit Card
UMTS	Universal Mobile Telecommunications System
VAS	Value-added Service

SUMÁRIO

1 INTRODUÇÃO

Os cartões (U)SIM passaram por diversas mudanças nas últimas décadas, o que fez com que a tecnologia se tornasse cada vez mais importante para a rotina das pessoas – e, consequentemente, mais atrativa para o mercado. Os aspectos técnicos dessas transformações foram abordados nesse trabalho, mas vale adiantar brevemente o contexto em que esses dispositivos estão inseridos.

Antigamente, os cartões SIM eram produzidos com sistemas operacionais proprietários. Foi apenas após a introdução do UICC, uma tecnologia avançada de Smart Card para telecomunicação, que esse cenário mudou. O sistema operacional e a plataforma física e lógica dos cartões (U)SIM passaram a ser padronizados, gerando uma projeção especial para a importância do Java Card – sistema operacional utilizado para plataformas UICC.

Segundo o autor e cientista DU CASTEL (2008), que assistiu de perto o surgimento do Java Card, foi nesse momento que os estudiosos da área entenderam que o mundo estava prestes a mudar – vale dizer que a visão deles não estava errada. Quando o mercado passou a padronizar o Java Card como o sistema operacional de um UICC, a interoperabilidade começou a ser possível. Dessa forma, as aplicações deixaram de ser proprietárias, o que abriu espaço para um novo modelo de negócio.

A linguagem Java era muito conhecida e suas aplicações podiam ser usadas em qualquer Smart Card que rodasse o seu sistema. Resumidamente, qualquer empresa que se disponibilizasse a entender o universo do cartão (U)SIM e decidisse explorar o Java poderia criar aplicações e vender para as empresas que de fato produzem os cartões.

Essa movimentação positiva fez com que a tecnologia avançasse e se transformasse no que é hoje: uma facilitadora cada vez mais veloz e eficiente para a comunicação das pessoas ao redor do mundo. Porém, obter uma boa compreensão sobre todas as normas, padrões, estruturas e aplicações relacionadas aos cartões (U)SIM não é tão simples quanto parece, embora a tecnologia seja extremamente presente no cotidiano da sociedade e mereça uma atenção extra.

1.1 OBJETIVO

Como um material de apresentação sobre os cartões (U)SIM, esse trabalho tem o objetivo de compilar as informações mais importantes para quem tem interesse em começar a estudar o assunto. Durante as pesquisas em busca de referências, foi possível perceber que muito material se encontra disperso pela internet, o que acaba dificultando o acesso a esse universo. Além disso, as normas podem ser consideradas complexas e não amigáveis para passageiros de primeira viagem. Por meio de um compilado geral sobre (U)SIM, comandos APDU e processos de autenticação, o foco é ajudar na criação de um conteúdo introdutório que pode servir como base informativa para aqueles que têm o interesse em se aprofundar na temática futuramente.

1.2 JUSTIFICATIVA

O avanço tecnológico fez com que os cartões (U)SIM se tornassem cada vez mais importantes na vida das pessoas. Segundo um levantamento feito pela FGV (2022), o Brasil tem, atualmente, mais de um smartphone por habitante. São 242 milhões de celulares inteligentes em uso no país, que tem pouco mais de 215 milhões de habitantes, de acordo com dados recentes do IBGE (2022).

No contexto mundial, um relatório produzido pela BUYSHARES (2021) mostra que, no ano estudado, existiam cerca de 3,6 bilhões de usuários de smartphones no mundo. A previsão da plataforma para 2023 é chegar no marco de 4,3 bilhões.

A grande parte destes aparelhos está conectada à rede por meio do (U)SIM, o que demonstra bem o quanto sua tecnologia impacta na sociedade. É a partir desses cartões que as pessoas conseguem se comunicar sem dar importância para a distância que as separam. Nas grandes capitais, é quase impossível lembrar de um mundo em que o acesso às redes não exista.

Principalmente hoje, após dois anos da pandemia de Covid-19, uma crise sanitária que fez com que muitas pessoas tivessem que estudar e trabalhar de dentro de casa, é explícito o quanto esse acesso é impactante. Por trás de tudo isso, no entanto, há muito estudo para que a tecnologia se aperfeiçoe cada vez mais. Entender o funcionamento e as estruturas básicas que formam os cartões (U)SIM faz parte da valorização desse estudo e do incentivo para que a área cresça e avance.

1.3 ESTRUTURA DO TRABALHO

O trabalho foi dividido em seis capítulos e dois apêndices. No Capítulo 1, há o texto introdutório com a contextualização do assunto. Já no Capítulo 2, os conceitos iniciais são abordados para que haja a construção de uma base de aprofundamento. É nesse tópico que se discorre sobre as definições de termos como Smart Card, SIM nativo, UICC e cartão (U)SIM, por exemplo. No Capítulo 3, com uma bagagem já formada sobre o assunto, apresenta-se a estrutura de arquivos e suas principais características. No Capítulo 4, um compilado sobre o APDU, enquanto o Capítulo 5 aborda as questões em torno do SIM Toolkit. Finalmente, o último capítulo discorre sobre a autenticação em redes 2G e 3G. Já nos apêndices, o primeiro explica sobre o algoritmo de Luhn e o segundo apresenta um exemplo de programa em Python para envio de comandos APDU.

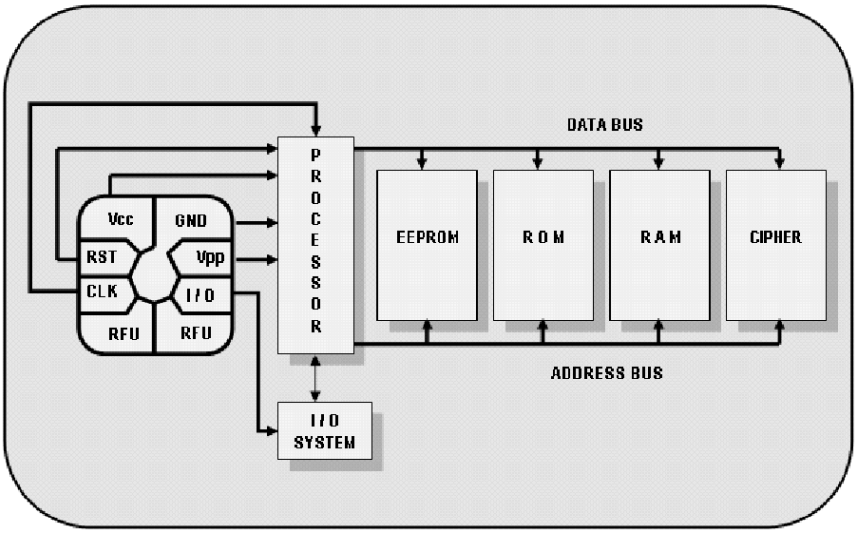
2 CONCEITOS INICIAIS

2.1 SMART CARD

O Smart Card é um cartão de plástico que possui um circuito integrado embutido em sua estrutura. Esse circuito pode ser apenas uma memória, sendo utilizado para armazenar informações, ou pode ser um microcontrolador – mais utilizado atualmente –, agregando a capacidade de realizar cálculos, autenticações e executar sistemas operacionais e aplicações.

Além de suas características físicas, ele também assume o papel de uma identificação eletrônica, podendo armazenar informações como dados pessoais e chaves de segurança, tendo, inclusive, a capacidade de realizá-la de forma criptografada e tornando-se um produto seguro e confiável.

Figura 1 - Arquitetura de um Smart Card



Fonte: Magiera (2006).

A Figura 1 é um exemplo típico da estrutura de um Smart Card utilizado para os setores de cartões (U)SIM e cartões bancários. A sua arquitetura mais comum é composta por vários componentes internos, como processador, memória EEPROM, ROM e RAM, além de um coprocessador de criptografia. O sistema operacional – Java Card e Multos são os mais conhecidos – é armazenado na memória ROM, enquanto a EEPROM é responsável pelo armazenamento de dados de aplicações e extensões do sistema operacional. A RAM é a memória utilizada para realizar operações. A comunicação entre o cartão e um dispositivo compatível é realizada através das portas I/O. O coprocessador de criptografia, por sua vez, é

responsável por processar cálculos envolvendo algoritmos de criptografia, garantindo assim a segurança das informações armazenadas e daquelas que serão transmitidas. (MAGIERA, 2006)

Essa ferramenta é amplamente utilizada em diferentes setores, como financeiro, telecomunicações, saúde e segurança, podendo conectar pessoas ao redor do mundo por meio de cartões (U)SIM, realizar transações bancárias com cartões de crédito e débito, e fornecer acesso a locais e dispositivos privados com crachás eletrônicos, por exemplo.

> O Smart Card, graças à sua portabilidade, ao seu poder de conexão com as redes, à sua segurança intrínseca e à sua memória protegida, permite-nos confidenciar os nossos segredos mais profundos e nos representa no mundo digital. (DU CASTEL, 2008)

Nos últimos anos, essa ferramenta tem sido fundamental para o desenvolvimento de um mundo virtual e inteligente, tornando-se cada vez mais importante para o avanço tecnológico.

2.2 SIM NATIVO

Historicamente, o termo “cartão SIM” é comumente usado para se referir a qualquer chip oferecido por uma operadora de telefonia. Tecnicamente, no entanto, esse termo se aplica a cartões que possuem características específicas.

Inicialmente, eles foram criados para permitir o acesso de usuários às redes GSM, e sua aplicação específica – NAA ou Network Access Application – era conhecida como SIM. Como esses cartões eram Smart Cards com apenas essa aplicação, eles passaram a ser conhecidos popularmente como cartões SIM.

A aplicação SIM era padronizada – atualmente ETSI TS 151 011 –, mas os módulos e sistemas operacionais eram propriedade das empresas que os produziam, o que impedia grande parte da interoperabilidade.

De forma resumida, os cartões que possuíam sistemas operacionais proprietários são hoje reconhecidos como cartões SIM nativos, que como tinham apenas a aplicação SIM, também se encaixam na categoria de cartões monoaplicação.

2.3 UNIVERSAL INTEGRATED CIRCUIT CARD

O UICC é uma tecnologia avançada e retrocompatível de Smart Card que foi projetada para substituir o SIM nativo e superar suas limitações. Ele é amplamente utilizado na indústria de telecomunicações e funciona como uma plataforma física e lógica para processar dados e redirecioná-los para diferentes aplicações, além de oferecer suporte para várias outras funcionalidades.

Uma das principais razões para o surgimento do UICC foi a necessidade de padronizar os módulos físicos e lógicos – encontrados hoje na norma ETSI TS 102 221.

O UICC é utilizado em conjunto com a tecnologia Java Card, um sistema operacional que propicia, entre outras coisas, a multiaplicação. Isso permitiu que diferentes NAAs, como USIM para UMTS – hoje também utilizado para LTE e NR –, SIM para GSM, e ISIM para IMS, por exemplo, pudessem ser utilizadas em um único módulo, armazenando chaves e informações necessárias para autenticação em suas respectivas redes.

Sua capacidade de armazenamento é maior comparada ao SIM nativo, tornando possível armazenar mais informações relevantes, como dados pessoais, informações de conta e outros dados importantes para o usuário e a operadora. Além disso, ele também oferece suporte para aplicações e serviços adicionais, bem como melhora a segurança e a privacidade dos usuários.

2.3.1 Java Card

Como descrito pela própria Oracle – desenvolvedora da tecnologia –, o Java Card permite que aplicações Java sejam executadas em dispositivos de pequeno porte, como os mencionados Smart Cards.

Algumas das vantagens e qualidades da tecnologia incluem:

- Interoperabilidade: aplicações Java Card, também conhecidas como Applets, podem ser executadas em vários dispositivos e plataformas – desde que a tecnologia esteja presente –, tornando-as mais flexíveis e escaláveis.
- Segurança: a tecnologia oferece uma série de mecanismos de segurança, como criptografia e proteção de acesso.
- Multiaplicação: cartões que possuem Java Card permitem que aplicações diferentes coexistam em um mesmo módulo.

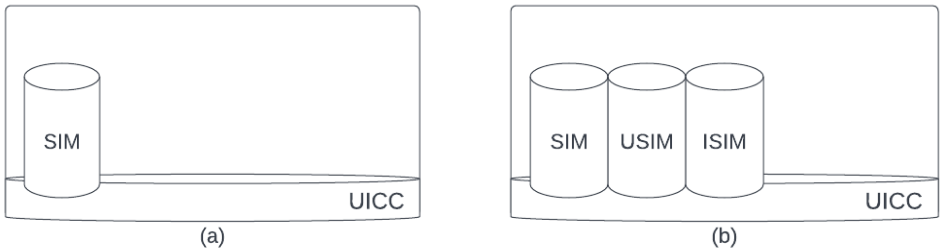
2.4 CARTÃO (U)SIM

O termo (U)SIM representa uma sigla universal que engloba todos os cartões formados por um módulo UICC, seja ele um cartão monoaplicação, com apenas a NAA do SIM, ou um cartão multiaplicação, com o SIM, USIM e ISIM presentes, por exemplo.

Entender este termo é importante para a definição e o entendimento das normas, visto que, em sua grande maioria, as especificações tendem a utilizá-lo como uma forma de dizer que as informações podem ser pertinentes a todos os cartões UICC que possuem uma aplicação presente – seja ela qual for.

Com isso, um (U)SIM pode ser um cartão monoaplicação como representado na imagem da Figura 2(a), ou um cartão multiaplicação, representado na Figura 2(b). A maior diferença entre este cartão (U)SIM monoaplicação e o cartão SIM nativo – que já caiu em desuso – seria a presença e a utilização da plataforma UICC e de todas as qualidades atreladas a ela.

Figura 2 – Arquitetura básica de cartões (U)SIM: (a) (U)SIM com monoaplicação; (b) (U)SIM com multiaplicação



Fonte: Autoria Própria.

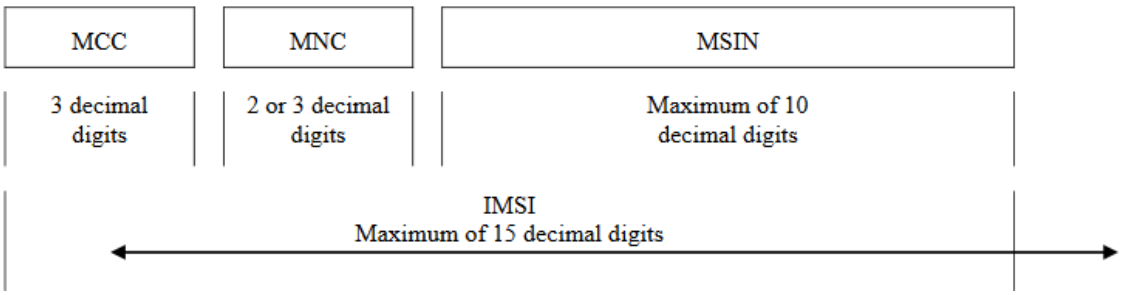
Em sua forma prática, ele é o cartão utilizado para armazenar as informações do usuário, como os números de identificação IMSI e ICCID, os dados e chaves de autenticação, e as configurações de rede. Ele também é essencial para garantir a privacidade e a segurança das comunicações realizadas por um assinante. De forma resumida, é o grande responsável por vincular o aparelho celular à rede de telefonia.

2.5 INTERNATIONAL MOBILE SUBSCRIBER IDENTITY

O International Mobile Subscriber Identity, mais conhecido como IMSI, é um número único, geralmente de 15 dígitos, que identifica exclusivamente cada usuário das redes móveis. Vinculado ao cartão (U)SIM, ele contém o código do país, o código da operadora associada à rede e o número de identificação do assinante móvel.

Ele é armazenado no cartão (U)SIM e no HLR – que é responsável por gerenciar as informações dos assinantes, incluindo suas credenciais de autenticação, números de telefone, status de conta e informações de localização. Esse valor é geralmente utilizado como o primeiro passo na autenticação em uma rede, onde o cartão (U)SIM se identifica utilizando o número IMSI. Isso permite a confirmação de que o (U)SIM realmente pertence à operadora e de que o usuário tem um plano ativo, autorizando assim sua conexão.

Figura 3 - Estrutura do IMSI



Fonte: ETSI TR 102 300-5 V1.4.1 (2015).

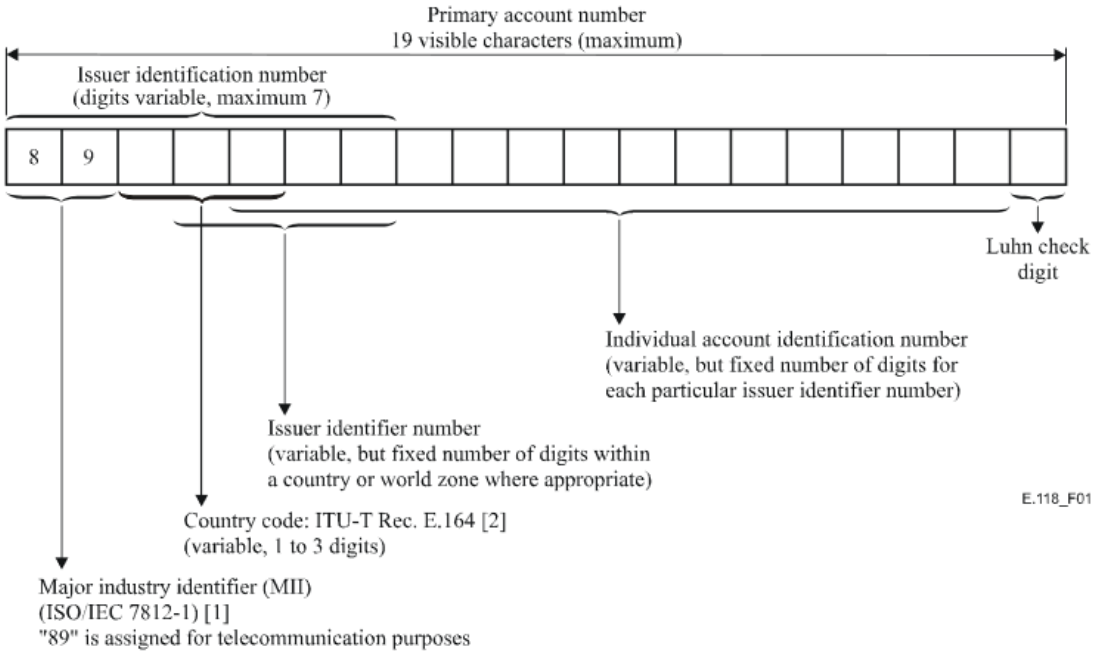
A estrutura de um número IMSI é definida de acordo com a Figura 3. Já o significado de cada elemento pode ser conferido a seguir:

- MCC: Mobile Country Code (código do país).
  - O valor definido para o Brasil é ‘724’.
- MNC: Mobile Network Code (código da rede móvel).
  - Principais valores conhecidos de operadoras no Brasil:
    - Claro: 05.
    - TIM: 02, 03, 04.
    - VIVO: 06, 10, 11, 23.
- MSIN: Mobile Subscriber Identification Number (número de identificação do assinante).

2.6 INTEGRATED CIRCUIT CARD IDENTIFIER

O ICCID é um número de série único que é atribuído a cada módulo UICC pelo seu emissor. Ele é composto por várias partes, incluindo o valor de identificação da indústria, o código do país, o código de identificação do emissor, o valor de identificação e, para finalizar, o dígito verificador.

Figura 4 - Estrutura do ICCID



Fonte: ITU-T Rec E.118 (2006).

- Identificação da indústria: este identificador é um valor de 1 byte definido pela ISO 7812. Para telecomunicações, é utilizado o valor ‘89’.
- Código do país: cada país possui um único código, que é definido e recomendado pela União Internacional de Telecomunicação – ITU. De acordo com a recomendação E.164, o valor definido para o Brasil é ‘55’.
- Código de identificação do emissor: normalmente contém o valor do MNC – número que identifica a operadora dentro de um país.
- Valor de identificação: após todos os valores pré-definidos, é este que irá de fato criar um valor único para cada ICCID, sendo usualmente sequencial e controlado pela operadora.
- Digito verificador: utiliza do algoritmo de Luhn – exemplificado no Apêndice A – para criar um código de checagem, permitindo a validação de valores ICCID.

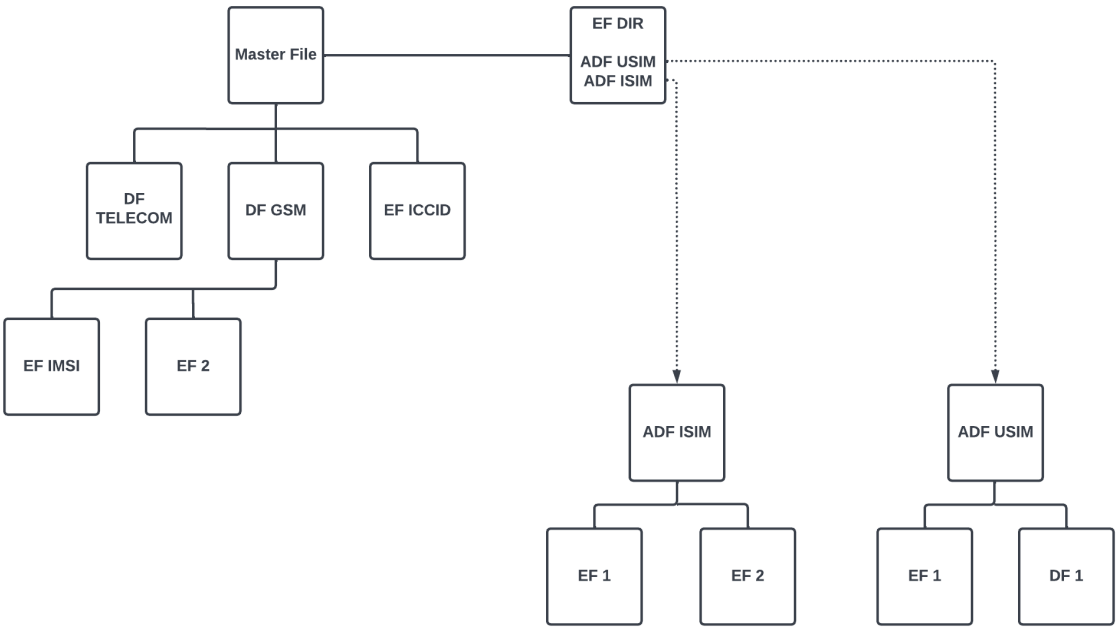
3 ESTRUTURA DE ARQUIVOS E PRINCIPAIS CARACTERÍSTICAS

Um cartão (U)SIM possui diversos arquivos com características e informações próprias que são organizados em uma estrutura definida e recomendada pela ETSI. Para a organização estrutural dos arquivos na plataforma UICC, nos basearemos na norma ETSI TS 102 221. Já para o conteúdo e as particularidades dos arquivos presentes nas aplicações, serão utilizadas as normas ETSI TS 151 011 – para a aplicação SIM –, ETSI TS 131 102 – para a aplicação USIM – e ETSI TS 131 103 – para ISIM.

3.1 ESTRUTURA DE ARQUIVOS

De acordo com a norma ETSI TS 102 221, é estabelecida uma estrutura recomendada para o armazenamento de dados dentro de uma plataforma UICC. É importante destacar que cartões multiaplicação terão suas NAAs adicionais – qualquer aplicação que não seja o SIM – fora da estrutura principal do arquivo raiz.

Figura 5 - Estrutura de arquivos de um (U)SIM



Fonte: Autoria Própria.

No caso da aplicação SIM, todos os arquivos referentes a ela estarão dentro da estrutura do diretório raiz, conhecido como Master File. Além do diretório raiz, podem existir estruturas de arquivos separadas para cada aplicação adicional presente no cartão, conhecidas como ADF.

Dessa forma, em um cenário hipotético com aplicações de USIM e ISIM, surgem outras duas estruturas de arquivos separadas da disposição principal do MF. Essas aplicações possuem seus identificadores AID armazenados em um arquivo chamado DIR, responsável por identificar e indicar à plataforma quais são as demais estruturas de arquivos.

3.2 CARACTERÍSTICAS GERAIS DOS ARQUIVOS

Cada arquivo tem uma gama de características – como tamanho, conteúdo, identificadores e condições de acesso.

3.2.1 Tipos de arquivos

Cada arquivo presente na estrutura de um (U)SIM terá seu próprio formato. Esses são descritos pela norma ETSI TS 102 221.

3.2.1.1 Master File (MF)

É o diretório raiz do principal sistema de arquivos de um (U)SIM, sendo o ponto de partida para todos os outros arquivos presentes nele.

3.2.1.2 Dedicated File (DF)

São diretórios que armazenam conjuntos de arquivos destinados a um propósito comum. Apesar de ser considerada uma aplicação, os arquivos de configurações GSM estarão presentes em um DF encontrado abaixo do diretório raiz – seguindo com as definições propostas antes da implementação do UICC.

3.2.1.3 Application Dedicated File (ADF)

Com a chegada da plataforma UICC, todas as novas aplicações que necessitam de uma estrutura de arquivos estarão presentes em um novo tipo de diretório, o ADF.

Ele é um tipo específico de Dedicated File utilizado exclusivamente para armazenar arquivos relacionados a uma aplicação. Os ADFs possuem a sua própria estrutura e são identificados pelo AID - código único que identifica cada aplicação.

Eles são diretórios independentes do MF, mas só podem ser acessados e corretamente identificados se o arquivo DIR presente no MF estiver configurado com seus valores de AID.

3.2.1.4 Elementary File (EF)

São arquivos capazes de armazenar informações e estarão inclusos dentro do MF e/ou em um (A)DF. Estes podem ser separados em quatro subtipos: Transparent File, Linear Fixed-Lenght Record File, Cyclic File e BER-TLV.

- Transparent File (TF): os TFs armazenam informações em uma sequência de bytes. São formados por um bloco de dados simples que pode ser acessado e manipulado como um todo ou parcialmente, usando operações com offset.

- Linear Fixed-Lenght Record File (LF): os LFs armazenam dados em forma de registros, que possuem o mesmo tamanho de dados e podem ser acessados individualmente.

- Cyclic File (CF): são arquivos que armazenam dados em forma de registros, assim como os LFs. No entanto, são armazenados em ordem cronológica e, quando o número máximo de dados é atingido, os registros mais antigos são automaticamente deletados para dar lugar aos mais recentes.
  Um exemplo de uso de arquivo cíclico é o arquivo EF LND (Last Number Dialled), que armazena informações sobre os últimos números discados. Como os registros mais antigos são automaticamente deletados, o arquivo LND permite que o usuário acesse rapidamente os números mais recentes sem precisar pesquisar na lista completa.

- Basic Encoding Rules - Tag-Length-Value (BER-TLV): é uma estrutura de codificação de dados utilizada para armazenar informações de diferentes tipos e tamanhos, além de permitir a adição de novos campos de dados sem a necessidade de mudar a estrutura do arquivo. Cada informação é codificada com um identificador (Tag), seguido pelo comprimento (Length) dos dados e, finalmente, pelo valor (Value) da informação. A estrutura BER-TLV permite que

os arquivos armazenem informações de forma estruturada e eficiente, facilitando a sua leitura e manipulação.

3.2.2 Identificadores de arquivos e aplicações

3.2.2.1 File IDentifier

Cada arquivo possui um identificador único conhecido como FID (File IDentifier), que tem um valor de 2 bytes e é utilizado para facilitar o reconhecimento deles. Sendo assim, quando comandos de leitura ou atualizações são enviados a um arquivo, podemos nos referir a ele pelo seu identificador.

Na Figura 6, por exemplo, é possível notar que o identificador de dois bytes do arquivo EF ICCID tem o valor de ‘2FE2’.

Figura 6 - Características do EF ICCID

Identifier: '2FE2'	Structure: transparent		Mandatory
SFI: Optional			
File size: 10 bytes		Update activity: low	
Access Conditions: READ ALW UPDATE NEV DEACTIVATE ADM ACTIVATE ADM			
Bytes	**Description**	**M/O**	**Length**
1 to 10	Identification number	M	10 bytes

Fonte: ETSI TS 102 221 V17.3.0 (2022).

3.2.2.2 Application IDentifier

O AID possui uma atuação semelhante, mas tem como foco a identificação de aplicações presentes dentro de um cartão (U)SIM. Sempre que há uma aplicação referente a USIM, também existe um AID para identificá-la. O mesmo acontece com o ISIM ou qualquer outro Applet presente no cartão.

Ele geralmente é composto por uma sequência de números hexadecimais com comprimento máximo de 16 bytes. Os primeiros 5 bytes são conhecidos como o "RID" (Registrator Identifier) – definidos na ISO/IEC 7816-4 –, que identifica o provedor da aplicação,

seguido pelo "PIX" (Progamm Identifier Extension), que identifica a aplicação específica dentro do provedor.

Figura 7 - Estrutura do AID

<---------- Application IDentifier (AID) ---------->	
Registered application provider IDentifier (RID)	Proprietary application Identifier eXtension (PIX)
<---------- 5 bytes ---------->	<---------- ≤11 bytes ---------->

Fonte: ETSI TS 101 220 V17.0.1 (2022).

Os valores de RID definidos pela norma são:

- 'A000000009' para ETSI;
- 'A000000087' para 3GPP.

3.2.3 Recursos de segurança (PIN e ADM)

Para proteger o acesso aos arquivos, a norma definiu alguns padrões de segurança, assim como a utilização de chaves que protegem as informações dos arquivos – tornando-os acessíveis apenas com a apresentação dela.

- PIN1 (Personal Identification Number 1): é um código de segurança pessoal composto por 4 a 8 dígitos, que é usado para proteger o acesso às informações confidenciais contidas no cartão (U)SIM. Quando ativo, ele é solicitado ao ligar o telefone ou quando o cartão (U)SIM é inserido em um dispositivo. Se o valor digitado for incorreto, o aparelho não poderá acessar as funcionalidades do cartão, incluindo a conexão com a rede.

- PIN2 (Personal Identification Number 2): é um código de segurança pessoal opcional, semelhante ao PIN1, mas é usado para proteger o acesso a certas funcionalidades do cartão (U)SIM. Ele é normalmente utilizado para limitar as chamadas por meio do FDN (Fixed Dialing Numbers), que permite realizar a chamada apenas para números presentes neste arquivo, sendo muito utilizado por empresas que distribuem celulares para funcionários e querem limitar o acesso.

- PUK (Personal Unblocking Key): é um código utilizado para desbloquear e resetar os valores de PIN1 ou PIN2 caso sejam inseridos incorretamente várias vezes. Cada PIN terá uma chave PUK individual.

- ADM (Administrative Key): é um código de administrador usado para gerenciar as configurações de segurança do cartão (U)SIM. Ele é geralmente utilizado pelas operadoras para garantir que as configurações de segurança sejam mantidas corretamente – sem alterações indesejadas.

3.2.3.1 Condições de acesso

As condições de acesso trabalham para que o arquivo tenha a possibilidade de aceitar ou negar um comando. Elas definem se será necessário apresentar algum tipo de chave para executar uma ação dentro do arquivo.

Por exemplo, na Figura 8, é possível observar as condições de acesso do arquivo FDN.

Figura 8 – Características do EF FDN

Identifier: '6F3B'	Structure: linear fixed		Optional
Record length: X+14 bytes		Update activity: low	
Access Conditions: READ PIN UPDATE PIN2 DEACTIVATE ADM ACTIVATE ADM			
Bytes	**Description**	**M/O**	**Length**
1 to X	Alpha Identifier	O	X bytes
X+1	Length of BCD number/SSC contents	M	1 byte
X+2	TON and NPI	M	1 byte
X+3 to X+12	Dialling Number/SSC String	M	10 bytes
X+13	Capability/Configuration2 Identifier	M	1 byte
X+14	Extension2 Record Identifier	M	1 byte

Fonte: ETSI TS 131 102 V17.8.0 (2023).

O Read define se o arquivo necessita da apresentação de alguma chave para a realização da leitura. No caso do FDN que está configurado com a leitura para PIN1 – e partindo do pressuposto que a chave esteja ativa –, será necessário apresentá-lo para ler o arquivo.

A condição de Update é utilizada para definir qual é a chave necessária para fazer a atualização do arquivo. Neste caso, será preciso apresentar a chave PIN2 para atualizar o arquivo FDN.

Para as condições de ativação e desativação do arquivo, no caso do FDN definidas como ADM, é apenas com a chave do administrador – de posse da operadora – que o arquivo pode ser ativado ou desativado, limitando acessos indesejados.

Outros valores de condições que também podem estar presentes são o ALWAYS e o NEVER. Como os próprios nomes representam na tradução literal, comandos com condições definidas para ALWAYS podem ser acessados sem a necessidade da apresentação de uma chave. Já aqueles definidos com NEVER não devem ser acessados nem mesmo pela própria operadora.

4 APPLICATION PROTOCOL DATA UNIT

Os comandos APDU – definidos na norma ETSI TS 102 221 – são usados para enviar solicitações de leitura, escrita e outras operações para o cartão (U)SIM durante a comunicação com um dispositivo compatível. O fluxo de comunicação normalmente é iniciado pelo dispositivo com um comando APDU – ou C-APDU –, seguido da resposta do cartão – R-APDU.

Os comandos APDU são compostos por um cabeçalho de 4 bytes e um corpo com até 257 bytes.

Figura 9 - Estrutura do C-APDU

Code	Length	Description	Grouping
CLA	1	Class of instruction	Header
INS	1	Instruction code	
P1	1	Instruction parameter 1	
P2	1	Instruction parameter 2	
Lc	0 or 1	Number of bytes in the command data field	Body
Data	Lc	Command data string	
Le	0 or 1	Maximum number of data bytes expected in response of the command	

Fonte: ETSI TS 131 102 V17.8.0 (2023).

Para configurar um comando APDU, é necessário especificar o código de classe, o código de instrução e os parâmetros opcionais, bem como os dados que serão transmitidos ou solicitados. Dependendo do tipo de solicitação e da quantidade de dados que estão sendo transmitidos, o tamanho real de um comando APDU pode variar.

4.1 ESTRUTURA DO C-APDU

A estrutura de um C-APDU é separada em duas partes, como mostrado na Figura 9: o cabeçalho e o corpo do comando.

4.1.1 Cabeçalho de um C-APDU

O Class Instruction (CLA) é um valor de 1 byte que especifica a classe do C-APDU. Ele é usado para identificar o conjunto de instruções ao qual o C-APDU pertence e para determinar como o comando deve ser tratado pelo dispositivo alvo.

O valor do parâmetro CLA é determinado pelo primeiro nibble do byte, enquanto o segundo nibble é usado para indicar o canal de comunicação a ser utilizado.

Para telecomunicação, o valor de ‘0x’ foi definido para o uso de comandos por meio da plataforma UICC, enquanto o ‘Ax’ é utilizado para acessar arquivos visíveis pela aplicação SIM – esta classe se manteve como legado da antiga definição.

Figura 10 - Codificação do byte CLA para canais lógicos padrões

b8	b7	b6	b5	b4	b3	b2	b1	Value	Meaning
0	0	0	0	-	-	-	-	'0X'	The coding is according to the first interindustry values of CLA byte defined in ISO/IEC 7816-4 [12]
1	0	1	0	-	-	-	-	'AX'	Coded as for '0X' unless stated otherwise
1	0	0	0	-	-	-	-	'8X'	Structured as for '0X', coding and meaning is defined in the present document
-	-	-	-	X	X	-	-	-	Secure Messaging indication (see table 10.4)
-	-	-	-	-	-	X	X	-	Logical channel number from 0 to 3 (see clause 10.3)

Fonte: ETSI TS 102 221 V17.3.0 (2022).

O Instruction Code (INS) é um valor de 1 byte que indica o código da instrução a ser executada. A instrução nada mais é que o comando que de fato queremos utilizar em um arquivo, como selecionar, ler, atualizar, entre outros disponíveis de acordo com a Figura 11 – definida para a plataforma UICC – e a Figura 12 – definida para a aplicação SIM.

Figura 11 - Instruções definidas para a plataforma UICC

COMMAND	CLA	INS
Command APDUs		
SELECT FILE	'0X' or '4X' or '6X'	'A4'
STATUS	'8X' or 'CX' or 'EX'	'F2'
READ BINARY	'0X' or '4X' or '6X'	'B0'
UPDATE BINARY	'0X' or '4X' or '6X'	'D6'
READ RECORD	'0X' or '4X' or '6X'	'B2'
UPDATE RECORD	'0X' or '4X' or '6X'	'DC'
SEARCH RECORD	'0X' or '4X' or '6X'	'A2'
INCREASE	'8X' or 'CX' or 'EX'	'32'
RETRIEVE DATA	'8X' or 'CX' or 'EX'	'CB'
SET DATA	'8X' or 'CX' or 'EX'	'DB'
VERIFY PIN	'0X' or '4X' or '6X'	'20'
CHANGE PIN	'0X' or '4X' or '6X'	'24'
DISABLE PIN	'0X' or '4X' or '6X'	'26'
ENABLE PIN	'0X' or '4X' or '6X'	'28'
UNBLOCK PIN	'0X' or '4X' or '6X'	'2C'
DEACTIVATE FILE	'0X' or '4X' or '6X'	'04'
ACTIVATE FILE	'0X' or '4X' or '6X'	'44'
AUTHENTICATE	'0X' or '4X' or '6X'	'88', '89'
GET CHALLENGE	'0X' or '4X' or '6X'	'84'
TERMINAL CAPABILITY	'8X' or 'CX' or 'EX'	'AA'
TERMINAL PROFILE	'80'	'10'
ENVELOPE	'80'	'C2'
FETCH	'80'	'12'
TERMINAL RESPONSE	'80'	'14'
MANAGE CHANNEL	'0X' or '4X' or '6X'	'70'
MANAGE SECURE CHANNEL	'0X' or '4X' or '6X'	'73'
TRANSACT DATA	'0X' or '4X' or '6X'	'75'
SUSPEND UICC	'80'	'76'
GET IDENTITY	'8X' or 'CX' or 'EX'	'78'
Transmission oriented APDUs applying to the above commands		
GET RESPONSE	'0X' or '4X' or '6X'	'C0'

Fonte: ETSI TS 102 221 V17.3.0 (2022).

Figura 12 - Instruções definidas para a aplicação SIM

COMMAND	INS	P1	P2	P3	S/R
SELECT	'A4'	'00'	'00'	'02'	S/R
STATUS	'F2'	'00'	'00'	lgth	R
READ BINARY	'B0'	offset high	offset low	lgth	R
UPDATE BINARY	'D6'	offset high	offset low	lgth	S
READ RECORD	'B2'	rec No.	mode	lgth	R
UPDATE RECORD	'DC'	rec No.	mode	lgth	S
SEEK	'A2'	'00'	type/mode	lgth	S/R
INCREASE	'32'	'00'	'00'	'03'	S/R
VERIFY CHV	'20'	'00'	CHV No.	'08'	S
CHANGE CHV	'24'	'00'	CHV No.	'10'	S
DISABLE CHV	'26'	'00'	'01'	'08'	S
ENABLE CHV	'28'	'00'	'01'	'08'	S
UNBLOCK CHV	'2C'	'00'	see note	'10'	S
INVALIDATE	'04'	'00'	'00'	'00'	-
REHABILITATE	'44'	'00'	'00'	'00'	-
RUN GSM ALGORITHM	'88'	'00'	'00'	'10'	S/R
SLEEP	'FA'	'00'	'00'	'00'	-
GET RESPONSE	'C0'	'00'	'00'	lgth	R
TERMINAL PROFILE	'10'	'00'	'00'	lgth	S
ENVELOPE	'C2'	'00'	'00'	lgth	S/R
FETCH	'12'	'00'	'00'	lgth	R
TERMINAL RESPONSE	'14'	'00'	'00'	lgth	S

Fonte: ETSI TS 151 011 V4.15.0 (2005).

Os parâmetros P1 e P2 são dois valores de 1 byte cada utilizados para indicar informações e configurações adicionais a uma instrução. Para o comando Select, por exemplo, podemos definir qual o identificador que utilizaremos para fazer a seleção. De acordo com a norma ETSI TS 102 221, o Select pode ter as seguintes características definidas na Figura 13 para P1 e na Figura 14 para P2.

Figura 13 - Definição do parâmetro P1 para o comando Select

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	0	0	0	0	0	Select DF, EF or MF by file id
0	0	0	0	0	0	0	1	Select child DF of the current DF
0	0	0	0	0	0	1	1	Select parent DF of the current DF
0	0	0	0	0	1	0	0	Selection by DF name (see note)
0	0	0	0	1	0	0	0	Select by path from MF
0	0	0	0	1	0	0	1	Select by path from current DF
NOTE: This is selection by AID.								

Fonte: ETSI TS 102 221 V17.3.0 (2022).

Figura 14 - Definição do parâmetro P2 para o comando Select

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
-	X	X	-	-	-	-	-	Application session control (see note 2)
-	0	0	-	-	-	-	-	- Activation/Reset
-	1	0	-	-	-	-	-	- Termination
0	-	-	0	0	1	-	-	Return FCP template
0	-	-	0	1	1	-	-	No data returned
-	-	-	-	-	-	X	X	Selection by AID control
-	-	-	-	-	-	0	0	- First or only occurrence
-	-	-	-	-	-	0	1	- Last occurrence
-	-	-	-	-	-	1	0	- Next occurrence
-	-	-	-	-	-	1	1	- Previous occurrence
NOTE 1: Whether the FCP information is returned or not depends on the type of APDU. NOTE 2: This only applies when P1 indicates SELECT by DF name.								

Fonte: ETSI TS 102 221 V17.3.0 (2022).

4.1.2 Corpo de um C-APDU

O Length of command data field (Lc) é um valor de 1 byte que indica, em bytes, o tamanho do dado presente no corpo do comando.

O Data field (DATA) é um valor de até 255 bytes que pode ser usado para enviar dados ou informações adicionais para uma instrução. Este campo pode conter dados para atualizar um arquivo ou o valor de FID/AID que você deseja selecionar, por exemplo.

Length of response data field (Le) é um valor de 1 byte que é usado para definir o tamanho máximo da resposta do cartão, permitindo que o dispositivo que enviou o comando APDU saiba quantos bytes devem ser lidos na resposta.

4.2 ESTRUTURA DO R-APDU

A R-APDU é um conjunto de dados enviado pelo cartão (U)SIM como resposta a um C-APDU enviado por um dispositivo. Ela é composta por um corpo opcional – que pode conter uma string de dados – e por 2 bytes de Status Word obrigatórios, que informam o resultado da operação realizada pelo cartão.

Figura 15 - Estrutura do R-APDU

Code	Length	Description
Data	Lr	Response data string
SW1	1	Status byte 1
SW2	1	Status byte 2

Fonte: ETSI TS 102 221 V17.3.0 (2022).

O Data field (DATA) é um campo opcional que pode conter dados retornados pelo dispositivo como resposta ao comando APDU. O tamanho deste campo é delimitado pelo valor especificado no parâmetro Le do C-APDU.

O SW1 e SW2 são 2 bytes que informam o status da execução do comando APDU. Eles podem indicar sucesso ou falha na operação, bem como fornecer mais informações sobre o erro ocorrido.

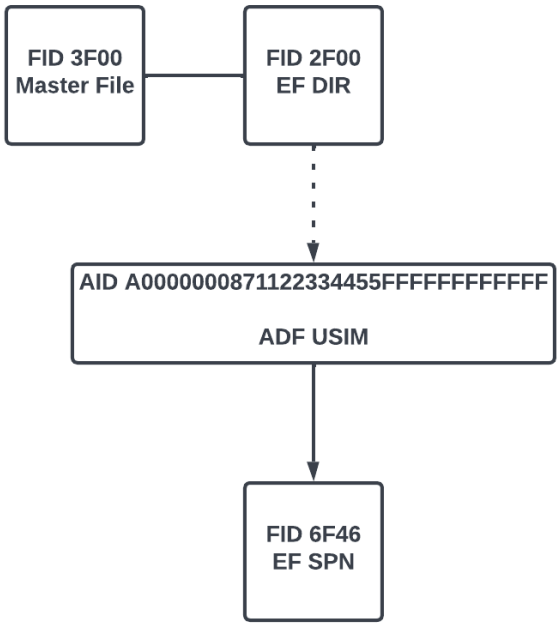
Os principais Status Word podem ser encontrados no Anexo A – valores retirados da norma ETSI TS 102 221.

4.3 ENVIO DE COMANDOS APDU - EXEMPLO

Com o auxílio de uma leitora externa, é possível utilizar o script produzido – Apêndice B – para enviar comandos APDU a um Smart Card. Como exemplo, será apresentado o processo de leitura do EF SPN, arquivo responsável por armazenar o nome da operadora que fornece o cartão (U)SIM.

Para o seguinte exemplo, será utilizado um cartão configurado manualmente com a finalidade demonstrativa. Porém, visto que o arquivo SPN possui a condição de leitura em ALWAYS, o teste poderia ser realizado em qualquer cartão obtido de uma operadora.

Figura 16 - Estrutura de arquivos para exemplo de envio de comandos APDU



Fonte: Autoria Própria.

Utilizando a estrutura da Figura 16 como exemplo, foram gerados os comandos APDU da Figura 17, Figura 18 e Figura 19, que serão enviadas ao cartão em sequência.

Figura 17 - Comando APDU para selecionar o ADF USIM

CLA	INS	P1	P2	Lc	DATA
00	A4	04	0C	10	A0000000871122334455FFFFFFFFFF
Utilizando a classe definida para a plataforma UICC.	Instrução SELECT.	Selecionando um arquivo pelo AID.	Não é necessário o retorno do template FCP.	Este comando possui 10 bytes no campo DATA.	AID da aplicação USIM.

Fonte: Autoria Própria.

Figura 18 - Comando APDU para selecionar o EF SPN

CLA	INS	P1	P2	Lc	DATA
00	A4	00	0C	02	6F46
Utilizando a classe definida para a plataforma UICC.	Instrução SELECT.	Selecionando um arquivo pelo FID.	Não é necessário o retorno do template FCP.	Este comando possui 2 bytes no campo DATA.	FID do arquivo SPN.

Fonte: Autoria Própria.

Figura 19 - Comando APDU para leitura de um TF com 17 bytes

CLA	INS	P1	P2	Le
00	B0	00	00	11
Utilizando a classe definida para a plataforma UICC.	Instrução READ BINARY.	Leitura sem Offset.		O comando lerá os 17 bytes do arquivo SPN.

Fonte: Autoria Própria.

Na Figura 20, é possível verificar que os três comandos foram enviados corretamente. Os dois primeiros retornaram o Status Word ‘90 00’, que representa que foi executado corretamente.

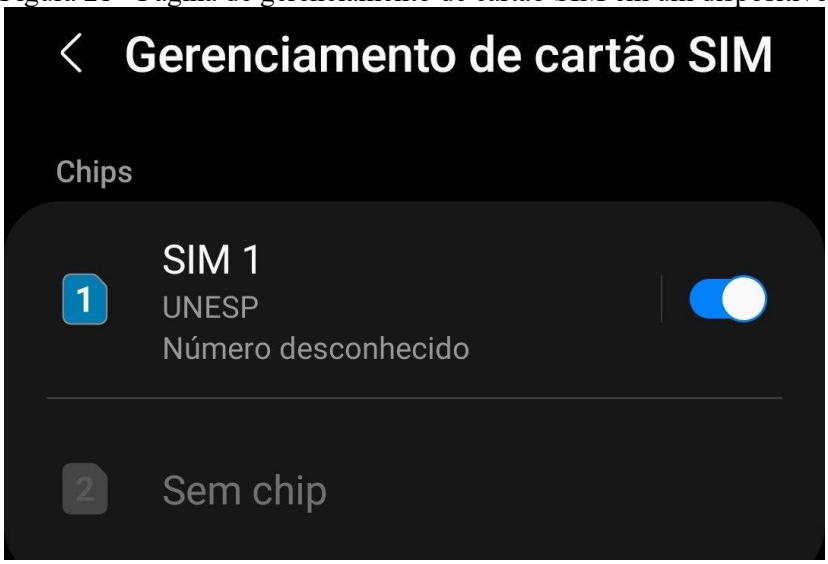
O terceiro comando, de READ BINARY, além de retornar o mesmo Status Word, também imprime os 17 bytes de resposta que foram declarados no C-APDU – o script imprime tanto em formato hexadecimal, como em ASCII. Sabe-se, então, que o conteúdo presente neste arquivo é o nome ‘UNESP’.

Figura 20 - Envio dos comandos APDU utilizando um script em Python

Fonte: Autoria Própria.

O SPN, como dito anteriormente, é responsável pelo armazenamento do nome da operadora. Como demonstrado na Figura 21, alguns dispositivos podem representá-lo dentro de sua página de gerenciamento de cartões.

Figura 21 - Página de gerenciamento de cartão SIM em um dispositivo



Fonte: Autoria Própria.

5 SIM TOOLKIT

O SIM Toolkit – especificado na norma ETSI TS 151 014 – ou CAT – especificado na norma ETSI TS 102 223 – é um conjunto de comandos que podem ser acionados por ações do usuário ou eventos da rede e, de forma resumida, definem como o cartão (U)SIM pode interagir com o mundo exterior. É esse conjunto de ferramentas que permeia a interação entre o aplicativo de rede e o usuário final, permitindo que o cartão inicie ações e que os usuários tenham acesso direto às funcionalidades prestadas pelas operadoras, como forma de serviços de valor agregado (VAS).

Seu papel é proativo, o que significa que a partir do recebimento de informações externas – sejam elas enviadas pelo usuário, pelo celular ou remotamente por um operador – ele iniciará um fluxo de envio de comandos. É nesse ponto que o conceito de evento determina quando o VAS será executado.

5.1 VALUE-ADDED SERVICE

O cartão (U)SIM também pode possuir em sua estrutura uma plataforma de serviços de valor agregado (VAS). Mais do que acessar a rede celular, o cliente consegue aproveitar tópicos de entretenimento, e-commerce e até gerenciamento de roaming e transações bancárias. Com a estratégia de apresentar um diferencial competitivo para o mercado, que vai além das funções convencionais de um cartão (U)SIM, o VAS existe como um caminho para reter clientes e, consequentemente, gerar mais renda.

5.2 CONCEITO DE EVENTO

O conceito de evento diz respeito a quando um VAS deve ser iniciado. Ele pode ser classificado em três tipos. São eles:

- Quando o usuário requer: entrando em um menu, o usuário pode acionar uma aplicação VAS, como, por exemplo, ativar o código de seleção de prestadora automático, ou mesmo consultar seu saldo.
- Quando o operador requer: um VAS pode ser iniciado pela operadora caso ela opte para que um aplicativo ou anúncio seja iniciado no (U)SIM do usuário, por exemplo.

- Quando algo acontece com o dispositivo: um VAS pode ser iniciado ao ligar um aparelho, ou mesmo quando sua posição geográfica é alterada.

Existem três tipos de comandos APDU especiais que representam os eventos descritos: comando ENVELOPE, STATUS e TERMINAL PROFILE – definidos nas normas ETSI TS 151 014 e ETSI TS 102 223.

O comando ENVELOPE pode enviar informações ao cartão (U)SIM sobre a maior parte dos eventos definidos anteriormente. Caso um usuário selecione uma aplicação por meio de um menu STK, por exemplo, será através de um comando ENVELOPE que esta mensagem será entregue ao cartão.

O comando STATUS é enviado constantemente pelo dispositivo – em uma frequência pré-definida – para verificar a presença do cartão. Dessa forma, o STK permite que se utilize deste comando como uma espécie de "clock" e, a cada X número de comando STATUS recebido, ele pode executar uma ação proativa.

O último comando a ser mencionado é o TERMINAL PROFILE. Este é recebido pelo cartão após a inicialização do dispositivo móvel. Isso permite que os desenvolvedores de aplicações STK utilizem dessa informação para executar comandos proativos ao ligar o aparelho.

5.3 SESSÃO PROATIVA

Quando o cartão recebe um comando de evento – seja ENVELOPE, STATUS ou TERMINAL PROFILE –, ele processa esta informação e, caso seja um evento que inicia alguma aplicação STK, envia uma mensagem ao ME dizendo que existe um comando proativo aguardando para ser executado.

Esta mensagem chega ao ME em formato de R-APDU, com um Status Word '91 xx' que representa que o cartão possui um comando proativo esperando para ser enviado ao dispositivo. Com isso, o aparelho terá a opção de aceitá-lo ou não – através de uma instrução chamada FETCH.

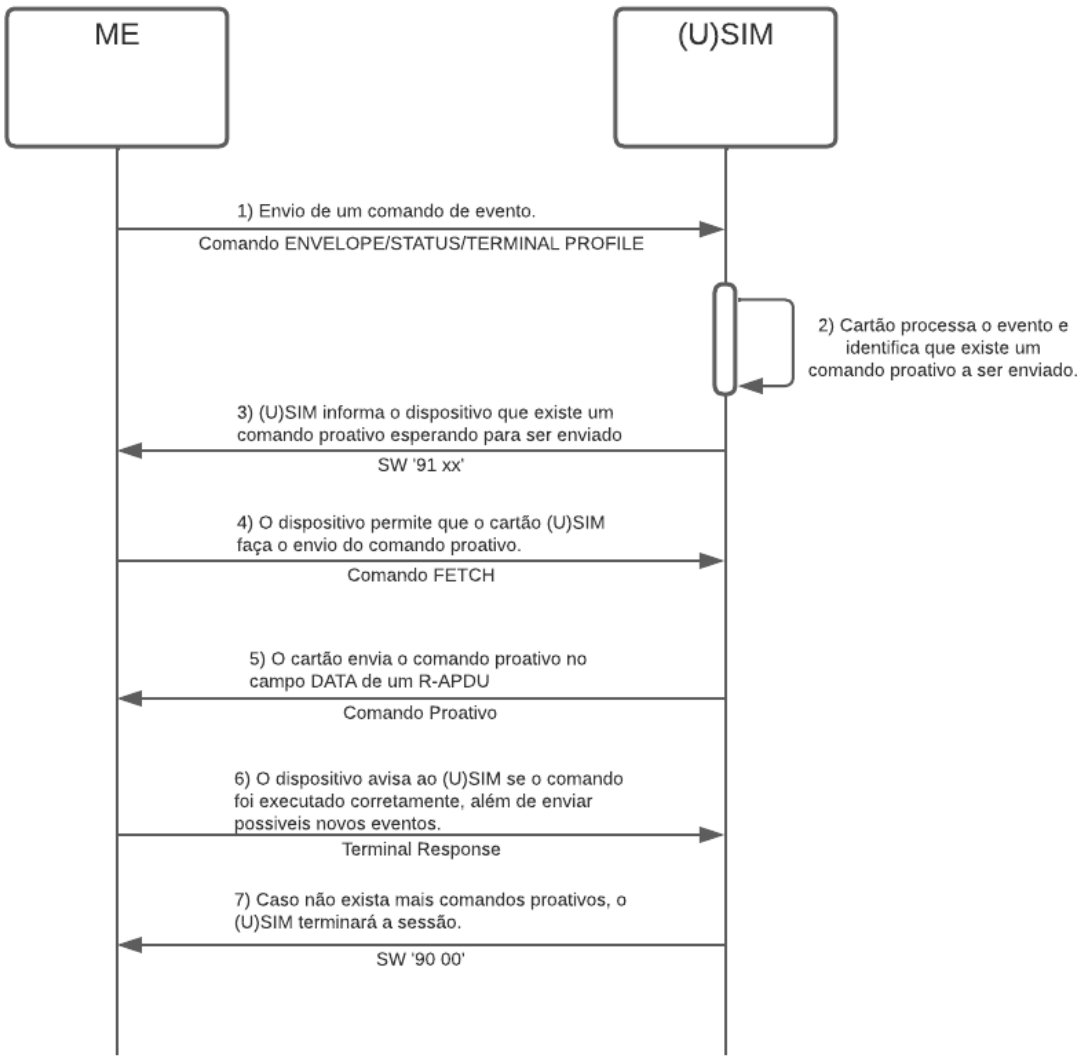
Caso o aparelho retorne a instrução FETCH, o cartão (U)SIM enviará um R-APDU, que dessa vez estará com o comando proativo incluso no campo DATA.

Sempre que houver o recebimento de um comando proativo, o dispositivo necessita enviar a informação de TERMINAL RESPONSE comunicando ao cartão se ele foi executado corretamente. Além disso, também anuncia se será preciso iniciar um novo ciclo.

Caso não existam mais comandos proativos para esta sessão, o cartão (U)SIM enviará um Status Word de ‘90 00’ para o ME.

Os passos dessa sessão podem ser visualmente observados na Figura 22.

Figura 22 - Fluxo de uma sessão proativa



Fonte: Autoria Própria.

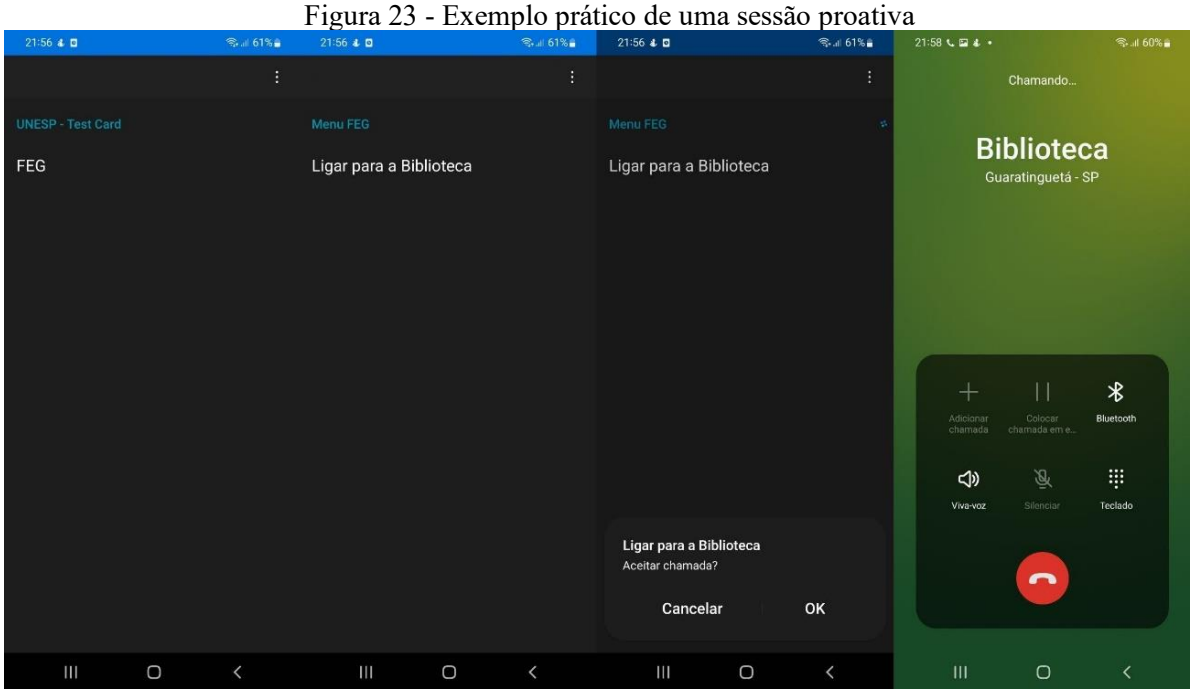
Um exemplo prático de uma sessão proativa é representado na Figura 23.

Quando selecionamos a primeira opção, “FEG”, o dispositivo envia um comando ENVELOPE ao (U)SIM dizendo que aquela aplicação foi selecionada. Após isso, o cartão retorna o comando proativo de SELECT ITEM pedindo para selecionarmos um novo item da lista.

Dentro deste menu, selecionamos o item “Ligar para a Biblioteca” e o dispositivo envia um novo comando ENVELOPE com esta informação. Agora, o cartão encaminha o comando proativo de SET UP CALL, e se inicia uma chamada com o número pré-definido.

Junto de uma outra gama de comandos proativos, o SELECT ITEM e o SET UP CALL também são definidos nas normas ETSI TS 151 014 e ETSI TS 102 223.

Figura 23 - Exemplo prático de uma sessão proativa



Fonte: Autoria Própria.

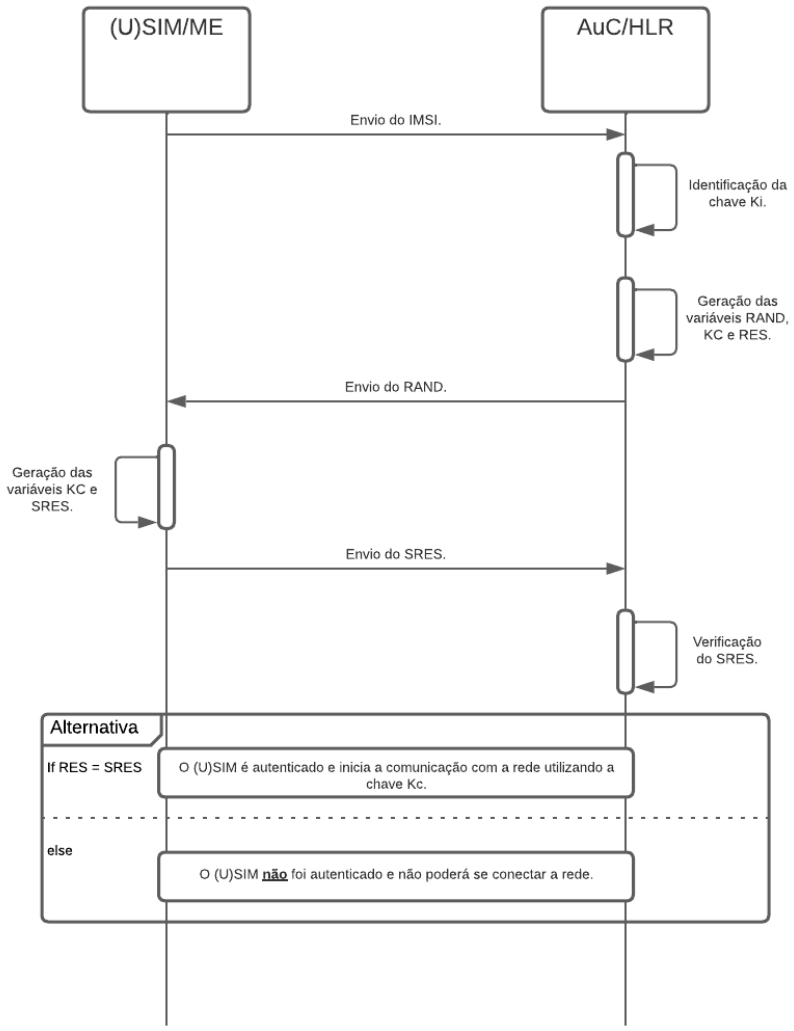
6 AUTENTICAÇÃO EM REDES

Neste capítulo, será apresentada uma visão especifica da autenticação em redes 2G e 3G, demonstrando o papel de um cartão (U)SIM neste processo. Por conta disso, elementos intermediários da rede não serão definidos.

6.1 AUTENTICAÇÃO 2G

O processo de autenticação 2G ocorre quando um dispositivo tenta se conectar a uma rede GSM. Durante esse processo, ocorrem trocas de variáveis entre o cartão (U)SIM e a rede.

Figura 24 - Fluxo de autenticação 2G



Fonte: Autoria Própria.

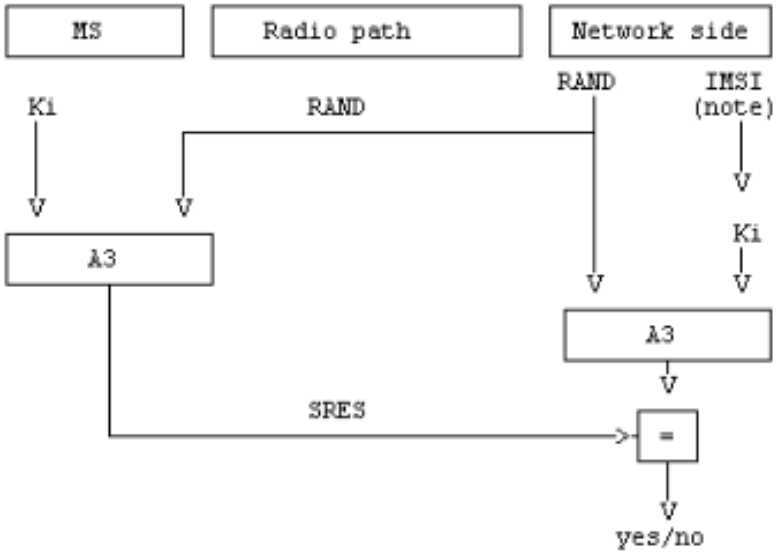
O início do processo se dá, de maneira geral, quando um dispositivo pretende se conectar a uma rede GSM. Neste momento, o (U)SIM disponibiliza o seu IMSI, que é enviado pelo ME para ser consultado no HLR.

O HLR é um banco de dados que armazena informações dos usuários vinculadas ao IMSI do (U)SIM. Com isso, a operadora pode verificar se há algum plano ativo e permitir que o dispositivo se conecte à rede.

Após uma análise positiva, o HLR notifica o AuC, que identifica o valor da chave de autenticação Ki relacionada a este IMSI. Com isso, inicia-se o processo de geração de uma variável randômica RAND. Posteriormente, com o algoritmo A3 apresentado na Figura 25, o valor RES é gerado. Utilizando o algoritmo A8 apresentado na Figura 26, gera-se também a chave de criptografia Kc. O AuC então envia essa mesma variável RAND para o SIM card, que realizará os mesmos cálculos para as variáveis SRES e KC.

Após este processo, o SIM card envia a variável SRES para o AuC, que verifica se ela é igual à variável RES. Caso positivo, o cartão (U)SIM é autenticado e tem permissão para se conectar à rede utilizando a chave Kc – usada tanto pelo dispositivo quanto pela rede – para criptografar e descriptografar dados trocados.

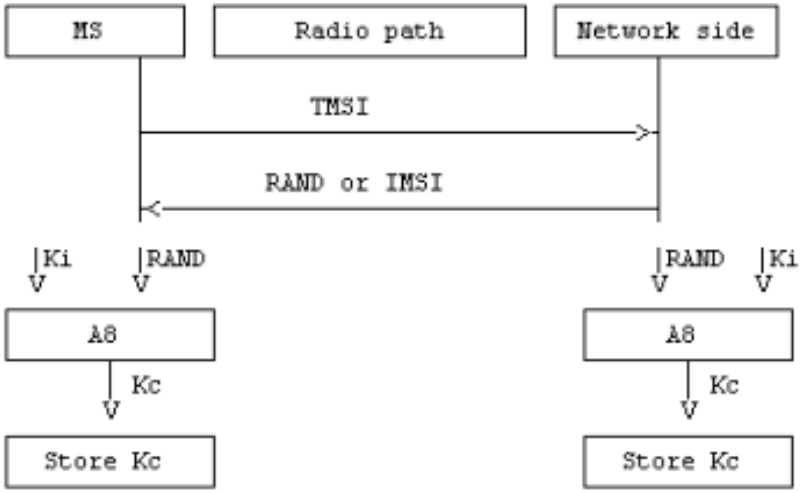
Figura 25 - Fluxo de verificação da variável SRES



NOTE: IMSI is used to retrieve Ki in the network.

Fonte: ETSI TS 143 020 V17.0.0 (2022).

Figura 26 - Fluxo de geração da variável Kc



Fonte: ETSI TS 143 020 V17.0.0 (2022).

Como mencionado, os valores de (S)RES e KC são calculados pelos algoritmos A3 e A8, respectivamente. Estes não são padronizados e as operadores são livres para escolher o método de cálculo, porém a norma recomenda a utilização do COMP128.

6.2 AUTENTICAÇÃO 3G

O processo de autenticação 3G ocorre quando um dispositivo pretende abrir conexão com uma rede UMTS. A principal vantagem em relação a autenticação na rede 2G é que, além da rede autenticar o cartão (U)SIM, agora o cartão também autenticará a rede.

Antes de definir o fluxo, primeiro é necessário entender o conceito da nova variável AUTN.

6.2.1 Authentication Token

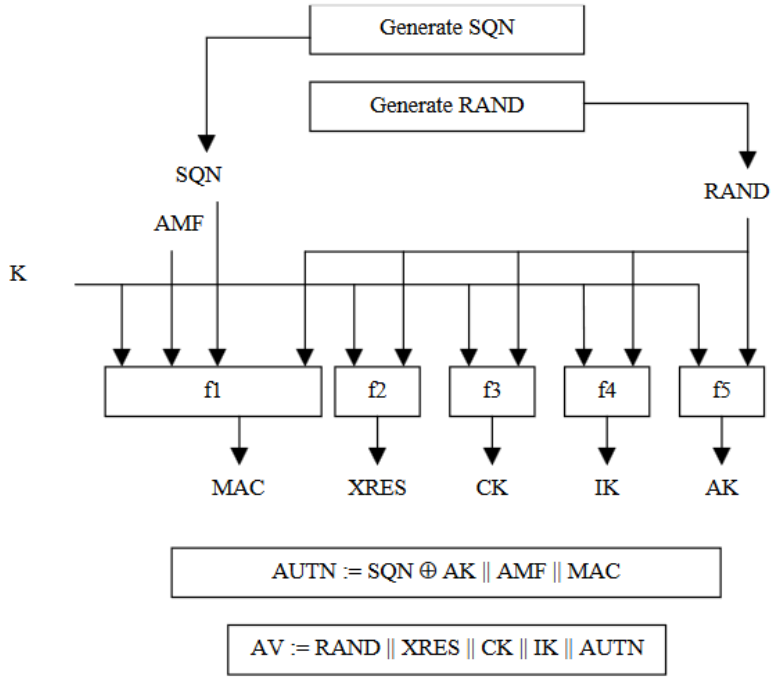
O Token de Autenticação é um mecanismo de segurança gerado pela rede de comunicação e enviado para o cartão (U)SIM. Ele é composto por três componentes distintos: SQN (Sequencial Number), AMF (Authentication Management Field) e MAC (Message Authentication Code).

O SQN é um número sequencial gerado pela rede. Ele é incrementado a cada nova autenticação, o que impede que ataques de replay sejam bem-sucedidos.

O AMF é um código que não é padronizado e pode, por exemplo, especificar quais algoritmos de criptografia devem ser utilizados na autenticação.

Por fim, o MAC é gerado pela rede com base nos valores de SQN, AMF, RAND e da chave de autenticação K – utilizando o algoritmo f1 como demonstrado na Figura 27. É ele que será utilizado pelo (U)SIM para fazer a autenticação da rede.

Figura 27 – Geração da AUTN e outras variáveis



Fonte: ETSI TS 133 102 V17.0.0 (2022).

A segurança do Token de Autenticação é crucial para garantir a confidencialidade e a integridade das comunicações e para evitar ataques.

6.2.2 Fluxo de autenticação 3G

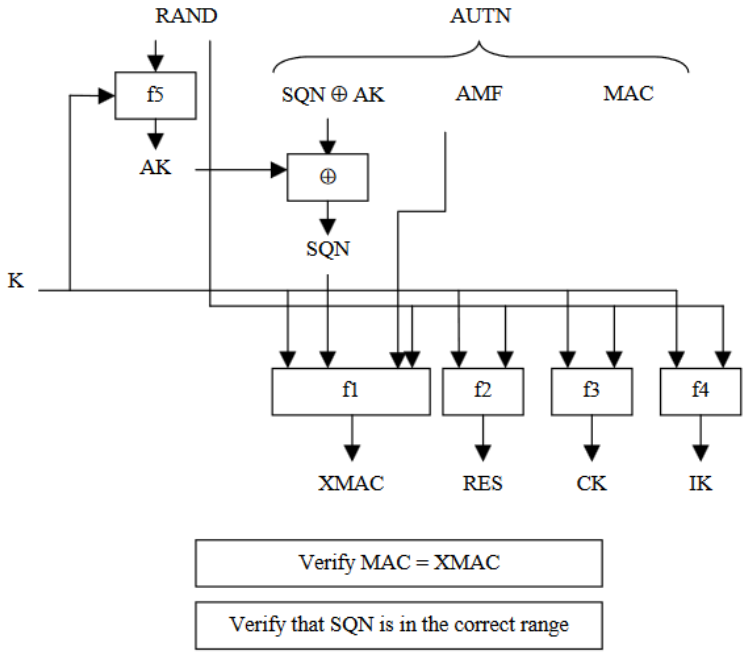
O início do fluxo ocorrerá também com o envio do valor do IMSI para a rede, que será consultado no HLR. Após a análise positiva, o HLR irá notificar o AuC, que dessa vez irá gerar o valor randômico RAND e o AUTN – como descrito anteriormente. Além disso, usará os algoritmos f2, f3 e f4 para gerar os elementos XRES – utilizado na autenticação do (U)SIM -, a chave CK de criptografia e a chave IK de integridade, respectivamente.

Os valores AUTN e RAND serão enviados ao (U)SIM, que através de um processo reverso – presente na Figura 28 –, poderá identificar quais são os valores específicos do AUTN. Com isso, poderá validar se o SQN está dentro do valor determinado – processo de verificação da sincronização – e se o MAC recebido é igual ao XMAC calculado – processo de autenticação.

Se tudo ocorrer corretamente, a rede está autenticada. O cartão então envia o valor de RES para a rede, que fará a comparação com o valor calculado por ela - o XRES. Caso os dois valores sejam iguais, isso significa que a rede também autenticou o usuário.

Com a dupla autenticação feita, o processo de troca de dados pode ser iniciado de maneira segura utilizando as chaves CK – para criptografia – e a chave IK – para integridade.

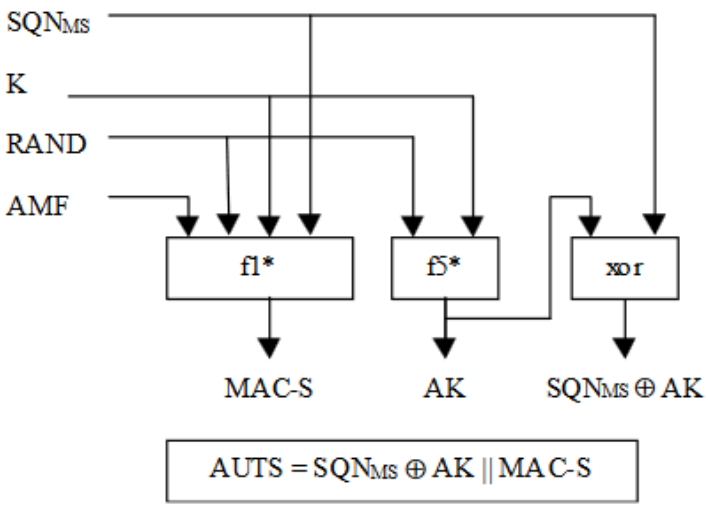
Figura 28 - Geração das variáveis de autenticação 3G no (U)SIM



Fonte: ETSI TS 133 102 V17.0.0 (2022).

Se durante o processo de validação da rede por parte do (U)SIM algum dos processos – sincronização ou autenticação – falhar, o valor do SQN presente na rede deverá ser ressincronizado. Para isso, o cartão irá gerar um novo token chamado AUTS. Este irá enviar a informação sobre qual foi o valor máximo de SQN já recebido pelo USIM – chamado de SQNms – que será utilizado para atualizar/ressincronizar os valores da rede. Além disso, no token também estará presente o valor do MAC-S, que permitirá que a rede identifique se o token foi realmente enviado pelo usuário.

Figura 29 - Geração do AUTS



Fonte: ETSI TS 133 102 V17.0.0 (2022).

Para o cálculo dos valores da Figura 28 e Figura 29, é recomendada a utilização do algoritmo Milenage.

7 CONCLUSÃO

A constante presença dos cartões (U)SIM na sociedade já foi abordada ao longo do trabalho, mas vale ressaltar novamente o seu papel para a relevância deste projeto. Embora o número de pessoas com um celular inteligente em mãos já seja alto no Brasil e no mundo, a tendência para os próximos anos é apenas aumentar, exigindo ainda mais da capacidade de conexão à rede que os cartões oferecem. Sendo assim, é essencial que a temática seja cada vez mais discutida para que avanços sejam feitos na área e mais profissionais se interessem pelo mercado.

Por mais que seja um caminho de estudo importante, muitas informações se encontram dispersas, o que dificulta a aproximação e o interesse de jovens profissionais e estudantes. Neste contexto, o foco do projeto foi a criação de um material introdutório e informativo sobre diversas questões que permeiam as características principais e o funcionamento de um cartão (U)SIM. Conforme mostrado, o assunto se torna mais compreensível quando as informações conversam entre si. Embora seja algo complexo, com muitas nuances, é por meio da exposição dos fatos que a temática se torna mais tátil.

A partir do texto introdutório e da exposição dos conceitos iniciais apresentados, foi possível se familiarizar com as definições de termos como Smart Card, Sim Nativo, UICC e Cartão (U)SIM, por exemplo. Após essa construção, o trabalho seguiu para a apresentação da estrutura de arquivos e das questões ligadas ao APDU e ao STK. Por fim, uma explicação sobre a autenticação em redes 2G e 3G, mais um tema que se aproxima diretamente do cotidiano e abre espaço para futuros estudos de redes mais complexas, como 4G e 5G.

Assim, conclui-se que o trabalho passou por todos os tópicos mais importantes para o entendimento inicial do universo (U)SIM. Com uma linha do tempo construída de forma cuidadosa, os capítulos seguem uma lógica de estudo que facilita o processo de aprendizagem e resolve a problemática das informações dispersas ligadas ao mercado. Ainda há mais para discutir sobre a tecnologia, mas este é um bom ponto para se iniciar.

REFERÊNCIAS

AUSSEL, J. D.; ROUSSEAU, L. **Pyscard user's guide**. [Paris: SourceForge, 2007]**.** Disponível em: https://pyscard.sourceforge.io/user-guide.html#pyscard-user-guide. Acesso em: 22 dez. 2022.

DU CASTEL, B. **Personal history of the Java Card.** Austin: Research Gate, 2008. Disponível em: https://www.researchgate.net/publication/259361072_Personal_History_of_the_Java_Card. Acesso em: 22 dez. 2022.

EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE. **T.S. 101 220**: smart cards; ETSI numbering system for telecommunication application providers. ver. 17.0.1. Sophia Antipolis: ETSI, 2022.

EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE. **T.S. 102 221:** smart cards; UICC-terminal interface; physical and logical characteristics. ver. 17.3.0. Sophia Antipolis: ETSI, 2022.

EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE. **T.S. 102 223**: smart cards; card application toolkit (CAT). ver. 17.1.0. Sophia Antipolis: ETSI, 2022.

EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE. **T.S. 131 102**: universal mobile telecommunications system (UMTS); LTE; 5G; characteristics of the universal subscriber identity module (USIM) application. ver. 17.8.0. Sophia Antipolis: ETSI, 2023.

EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE. **T.S. 133 102**: digital cellular telecommunications system (Phase 2+) (GSM); universal mobile telecommunications system (UMTS); LTE; 5G; 3G security; security architecture. ver. 17.0.0. Sophia Antipolis: ETSI, 2022.

EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE. **T.S. 143 020**: digital cellular telecommunications system (Phase 2+) (GSM); security related network functions. ver. 17.0.0. Sophia Antipolis: ETSI, 2022.

EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE. **T.S. 151 011:** digital cellular telecommunications system (Phase 2+); specification of the subscriber identity module - mobile equipment (SIM-ME) interface. ver. 4.15.0. Sophia Antipolis: ETSI, 2005.

EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE. **T.S. 151 014:** digital cellular telecommunications system (Phase 2+); specification of the SIM application toolkit for the subscriber identity module - mobile equipment (SIM - ME) interface. ver. 4.5.0. Sophia Antipolis: ETSI, 2004.

FUNDAÇÃO GETULIO VARGAS; **Pandemia acelerou processo de transformação digital das empresas no Brasil, revela pesquisa.** [Rio de Janeiro]: FGV, 2022. Disponível em: https://portal.fgv.br/noticias/pandemia-acelerou-processo-transformacao-digital-empresas-brasil-revela-pesquisa?utm_source=portal-fgv&utm_medium=fgvnoticias&utm_campaign=fgvnoticias-2021-05-26. Acesso em: 22 dez. 2022.

GILLIS, A. S. **Luhn algorithm.** [Tewksbury: Tech Target, 2022]. Disponível em: https://www.techtarget.com/searchsecurity/definition/LUHN-formula. Acesso em: 22 dez. 2022.

INTERNATIONAL TELECOMMUNICATION UNION. **E.118:** Overall network operation, telefone service, service operation and human factors – the international telecommunication charge card. Genebra: ITU, 2006.

INTERNATIONAL TELECOMMUNICATION UNION. **List of ITU-T recommendation E.164 assigned country codes.** Genebra: ITU, 2011.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. **Projeção da população do Brasil e das Unidades da Federação.** [Rio de Janeiro]: IBGE, 2023. Disponível em: https://www.ibge.gov.br/apps/populacao/projecao/. Acesso em: 23 jan. 2023.

KRIGER, D. **O que é Python, para que serve e por que aprender?** [Curitiba]: Kenzie Academy, 2022. Disponível em: https://kenzie.com.br/blog/o-que-e-python/ Acesso em: 22 dez. 2022.

MAGIERA, J.; PAWLAK, A. Security frameworks for virtual organizations. *In*: CAMARINHA-MATOS, L. M.; AFSARMANESH, H.; OLLUS, M (ed.). **Virtual organizations:** systems and practices. Berlim: Springer Science & Business Media, 2006. p. 133-148.

ORACLE. **Java Card:** The open application platform for secure elements. [Austin: Oracle, 2007]. Disponível em: https://www.oracle.com/docs/tech/java/java-card-data-sheet-19-01-07.pdf. Acesso em: 22 dez. 2022.

PASCUAL, R. **Smartphone subscriptions more than doubled in 5 years – 11% CAGR from 2016-2020.** [London]: BuyShares, 2022. Disponível em: https://buyshares.co.za/blog/2021/04/06/smartphone-subscriptions-more-than-doubled-in-5-years-11-cagr-from-2016-2020/. Acesso em: 22 dez. 2022.

APÊNDICE A – ALGORITMO DE LUHN

Desenvolvido por Hans Peter Luhn, da IBM, na década de 1960, o algoritmo de Luhn é uma fórmula matemática simples usada para validar os números de identificação de um usuário. De domínio público, ele pode ser usado por qualquer pessoa e foi projetado para detectar valores incorretos. Em Telecom, pode ser utilizado no ICCID, onde é utilizado para calcular o número de checagem e, posteriormente, fazer a validação dos valores. (GILLIS, 2022)

Considerando um valor exemplo de ICCID de 8955112233445566778X, em que 'X' é o valor de checagem, o algoritmo será definido pela lógica representada a seguir.

Todos os dígitos serão multiplicados um a um: o primeiro digito será multiplicado por dois, o segundo por um, o terceiro por dois, e assim por diante, de forma intercalada, formando a linha de valores R1.

Número ICCID	8	9	5	5	1	1	2	2	3	3	4	4	5	5	6	6	7	7	8
Fator multiplicativo	2	1	2	1	2	1	2	1	2	1	2	1	2	1	2	1	2	1	2
R1	16	9	10	5	2	1	4	2	6	3	8	4	10	5	12	6	14	7	16

Na linha R1, caso um valor possua dois dígitos, os mesmos deverão ser somados entre si, formando a linha de valores R2.

Número ICCID	8	9	5	5	1	1	2	2	3	3	4	4	5	5	6	6	7	7	8
Fator multiplicativo	2	1	2	1	2	1	2	1	2	1	2	1	2	1	2	1	2	1	2
R1	16	9	10	5	2	1	4	2	6	3	8	4	10	5	12	6	14	7	16
R2	7	9	1	5	2	1	4	2	6	3	8	4	1	5	3	6	5	7	7

Dessa maneira, agora é necessário aplicar os valores de R2 na equação (1), encontrando o valor de checagem X.

$$X = \left(10 - \left(\sum R_2 \bmod 10\right)\right) \bmod 10 \qquad (1)$$

Com isso, o valor de checagem X desse exemplo é 4. Completando o valor do ICCID – 89551122334455667784.

APÊNDICE B – PROGRAMA EM PYTHON PARA ENVIO DE APDU

Neste apêndice, há uma demonstração de como enviar comandos APDU com o auxílio de um script em Python.

O espaço de desenvolvimento utilizado na produção e teste dos scripts foi o Visual Studios, um ambiente de desenvolvimento integrado (IDE) que permite a criação de aplicações para diversos sistemas operacionais, além de suportar linguagens distintas, incluindo Pyhton. É nesse ambiente que ocorre a compilação e testagem dos programas.

Python

Python é uma linguagem de programação de alto nível – e é conhecida dessa forma por ser relativamente simples e de fácil compreensão. Idealizada pelo matemático holandês Guido Van Rossum, ela foi criada exatamente com o objetivo de otimizar a leitura de códigos e, ao longo dos anos, sua didática fez com que ganhasse popularidade entre os profissionais da indústria tecnológica. Considerada a linguagem mais usada no desenvolvimento web, um de seus maiores diferenciais é possuir muitas bibliotecas disponíveis livremente na internet com projetos e aplicações diversos. Isso cria um atalho para que os desenvolvedores tenham acesso a mais funcionalidades, gerando um ambiente colaborativo em torno da linguagem. (KRIGER, 2022)

Biblioteca pyscard

A biblioteca usada para o teste em questão foi a pyscard, um software livre que apresenta um conjunto de ferramentas e módulos desenvolvidos para Python e que permite o acesso a Smart Cards – incluindo cartões (U)SIM – através da API PC/SC. Ela fornece uma interface para enviar comandos APDU para cartões SIM e outros tipos de Smart cards, além de oferecer funções para gerenciar as informações armazenadas nos cartões. Resumidamente, a biblioteca facilita a visualização e torna todo o processo mais simples. A pyscard é compatível com a norma ISO 7816.

Para fazer a instalação da biblioteca, pode-se utilizar os seguintes comandos:

```
pip install --upgrade pip
pip install pyscard
pip install --upgrade pyscard
```

Código do programa de envio de APDU em Python

```
import smartcard

# Iniciar contador para identificar respostas
count = 1

# Definir o(s) comando(s) APDU através de uma entrada de dados do usuário
comandos_APDU = []
while True:
    apdu_str = input("Digite o comando APDU (ou mantenha em branco para terminar): ")
    if not apdu_str:
        break
    # Remover qualquer espaço recebido na entrada
    apdu_str = apdu_str.replace(" ", "")
    # Dividir a string recebida em uma lista de valores hexadecimais
    apdu_hex = [apdu_str[i:i+2] for i in range(0, len(apdu_str), 2)]
    # Converter os valores hexadecimais em inteiro - formato aceito pelo método 'transmit'
    apdu = [int(h, 16) for h in apdu_hex]
    # Adicionar a string no vetor de comandos
    comandos_APDU.append(apdu)

# Conectar-se a leitora de Smart Card
try:
    reader = smartcard.System.readers()[0]
    connection = reader.createConnection()
    connection.connect()
    print("\n" + "-" * 80)
    print ("Leitora conectada: %s" % reader)
    print("-" * 80)

# Mensagem de erro e encerramento do programa caso não seja detectado um cartão
except smartcard.Exception.NoCardException:
    print("Cartão não detectado.")
    exit()

# Enviar comandos APDU
for apdu in comandos_APDU:
    response, sw1, sw2 = connection.transmit(apdu)

    # Imprimir número da resposta
    print("Resposta %d" % count)
    count += 1
    # Imprimir resposta em Hexadecimal
    if response:
        print("Response data (hex):", " ".join(["{:02X}".format(b) for b in response]))
    # Imprimir resposta em ASCII
    if response:
        print("Response data (ASCII):", "".join([chr(b) if b >= 32 and b <= 126 else "." for b in response]))
    # Imprimir Status Word
    print("Status words: %02X %02X" % (sw1, sw2))
    # Imprimir separador
    if count > 1:
        print("-" * 80)

# Desconectar-se da leitora
connection.disconnect()
```

ANEXO A – PRINCIPAIS STATUS WORD

Table 10.7: Status byte coding - normal processing

SW1	SW2	Description
'90'	'00'	- Normal ending of the command
'91'	'XX'	- Normal ending of the command, with extra information from the proactive UICC containing a command for the terminal. Length 'XX' of the response data
'92'	'XX'	- Normal ending of the command, with extra information concerning an ongoing data transfer session

Table 10.8: Status byte coding - postponed processing

SW1	SW2	Error description
'93'	'00'	- SIM Application Toolkit is busy. Command cannot be executed at present, further normal commands are allowed

Table 10.9: Status byte coding - warnings

SW1	SW2	Description
'62'	'00'	- No information given, state of non-volatile memory unchanged
'62'	'81'	- Part of returned data may be corrupted
'62'	'82'	- End of file/record reached before reading Le bytes or unsuccessful search
'62'	'83'	- Selected file invalidated
'62'	'85'	- Selected file in termination state
'62'	'F1'	- More data available
'62'	'F2'	- More data available and proactive command pending
'62'	'F3'	- Response data available
'63'	'F1'	- More data expected
'63'	'F2'	- More data expected and proactive command pending
'63'	'CX'	- Command successful but after using an internal update retry routine 'X' times - Verification failed, 'X' retries remaining (see note)
NOTE:	For the VERIFY PIN command, SW1SW2 indicates that the command was successful but the PIN was not correct and there are 'X' retries left. For all other commands it indicates the number of internal retries performed by the card to complete the command.	

Table 10.10: Status byte coding - execution errors

SW1	SW2	Description
'64'	'00'	- No information given, state of non-volatile memory unchanged
'65'	'00'	- No information given, state of non-volatile memory changed
'65'	'81'	- Memory problem

Table 10.11: Status byte coding - checking errors

SW1	SW2	Description
'67'	'00'	- Wrong length
'67'	'XX'	- The interpretation of this status word is command dependent, except for SW2 = '00'
'6B'	'00'	- Wrong parameter(s) P1-P2
'6D'	'00'	- Instruction code not supported or invalid
'6E'	'00'	- Class not supported
'6F'	'00'	- Technical problem, no precise diagnosis
'6F'	'XX'	- The interpretation of this status word is command dependent, except for SW2 = '00'

Table 10.12: Status byte coding - functions in CLA not supported

SW1	SW2	Description
'68'	'00'	- No information given
'68'	'81'	- Logical channel not supported
'68'	'82'	- Secure messaging not supported

Table 10.13: Status byte coding - command not allowed

SW1	SW2	Description
'69'	'00'	- No information given
'69'	'81'	- Command incompatible with file structure
'69'	'82'	- Security status not satisfied
'69'	'83'	- Authentication/PIN method blocked
'69'	'84'	- Referenced data invalidated
'69'	'85'	- Conditions of use not satisfied
'69'	'86'	- Command not allowed (no EF selected)
'69'	'89'	- Command not allowed - secure channel - security not satisfied

Table 10.14: Status byte coding - wrong parameters

SW1	SW2	Description
'6A'	'80'	- Incorrect parameters in the data field
'6A'	'81'	- Function not supported
'6A'	'82'	- File not found
'6A'	'83'	- Record not found
'6A'	'84'	- Not enough memory space
'6A'	'86'	- Incorrect parameters P1 to P2
'6A'	'87'	- Lc inconsistent with P1 to P2
'6A'	'88'	- Referenced data not found

Table 10.15: Status byte coding - application errors

SW1	SW2	Error description
'98'	'50'	- INCREASE cannot be performed, max value reached
'98'	'62'	- Authentication error, application specific
'98'	'63'	- Security session or association expired
'98'	'64'	- Minimum UICC suspension time is too long
NOTE:	Applications may define their own error codes.	