Volume XXVII 2024
ISSUE no.2
MBNA Publishing House Constanta 2024

Scientific Bulletin of Naval Academy

SBNA PAPER • OPEN ACCESS

Modern protocols used in online card payments

To cite this article: Nicolae Nebancea and Ciprian Răcuciu, Scientific Bulletin of Naval Academy, Vol. XXVII 2024, pg. 53-62.

Submitted: 23.05.2024
Revised: 27.09.2024
Accepted: 07.10.2024

Available online at www.anmb.ro

ISSN: 2392-8956; ISSN-L: 1454-864X

doi: 10.21279/1454-864X-24-I2-005

Modern protocols used in online card payments

Nicolae Nebancea[1], Ph.D. Student

Eng. Ciprian Răcuciu[2], Prof. Ph.D.

[1]Military Technical Academy "Ferdinand I" – Systems Engineering for Defense and Security

[2]Titu Maiorescu University – Faculty of Informatics

Abstract. Recently, we have seen a dramatic increase in online payments for goods and services using bank cards or digital wallets, which is a clear indication that the near future is reserved for these types of payments. In the Eurozone alone, the total value of non-cash payments in mid-2022 amounted to 65.9 billion euros, of which 35.8 billion were card payments. However, the benefits of online payments do not come without risks and dangers, with the huge volumes of transactions acting as a magnet for cyber fraud. This study examines the benefits and limitations of the main protocols currently used for online card payment processing, providing detailed information on them and on alternatives tailored to the new threats that are emerging.

1. INTRODUCTION

The unprecedented development of the Internet has brought profound changes in the way human society interacts economically, with e-commerce being the most obvious result of these developments.

For most people, the term 'e-commerce' means shopping online on the World Wide Web. However, Electronic Commerce (E-Commerce) is more than the process of buying/selling products and services. It can encompass many other activities, such as: exchanges and negotiations between companies, internal company processes that companies carry out in support of buying/sourcing, selling, hiring, planning. E-commerce also involves the transfer of documents - from contracts or orders to images or voice recordings.

E-commerce can also be defined as buying or selling by via remote data transmission. This approach is specific to the marketing of commercial companies. Through the Internet a relationship of services and exchange of goods between the supplier and the prospective buyer.

In the 1990s, IBM, through an advertising campaign, also popularized the term equivalent Electronic Business. The term "e-business" was used to define the use of Internet technologies to improve and transform key processes in a business. In IBM's definition, e-business is a way of "providing secure, flexible and integrated access to run different businesses by combining the processes and systems that perform core business operations with those that make it possible to find information on the Internet" [1].

According to a report of European Central Bank published in 2022, total number of non-cash payments in the euro area in second half of 2022 increased by 8.8% to 65.9 billion compared with the previous six-month period, with total value rising by 2.8% to €118.8 trillion, from which card related payments accounted for 70% of total number of non-cash payments, Portugal having the largest share of card payments as a percentage of the total number of non-cash payments in the second half of 2022, at around 75% [2]. Worldwide, in 2022 we registered almost 625 billion transactions [3].

Of course, the accelerated digital evolution of the economy and society in recent years has created a wealth of opportunities, but has also brought new challenges, including threats, like credit card fraud. Year after year, credit card fraud attempts are on the rise, with a staggering 46% year-over-year increase reported globally. As credit card transactions continue to rise, the number of attempted fraud transactions follows suit. Online sellers, particularly e-commerce merchants, have become prime targets for fraudsters, experiencing a shocking 140% increase in credit card fraud attacks over the past three years. Global losses from payment cards currently totals $34 billion in 2022, the U.S. being the leader in credit card fraud with 36% of the total loss [4].

Credit card fraud can be divided into two main categories:

- Card-not-present (CNP) fraud
- Card-present fraud

Card-not-present (CNP) fraud is becoming more common as digital payments are now the norm. Once the fraudster obtains stolen credit card details, they can carry out multiple incidents of fraud, typically via online transactions. An example of digital CNP fraud is when a criminal makes very large online purchases or bulk purchases of the same item, acting quickly to maximize the time they have before the fraud is discovered.

CNP fraud represents 65% of all credit card fraud losses, highlighting the severity of the issue. This type of fraud primarily occurs in online transactions, phone payments, and manually entered card details, presenting fraudsters with ample opportunities to exploit vulnerabilities in less secure payment methods. Consumers and businesses must recognize the significance of this threat and implement robust security protocols to safeguard sensitive data during online transactions.

Card-present fraud is becoming less common thanks to the advent of chips and PIN. Such incidents that can lead to a card-present fraud, are credit card theft, credit card cloning (skimming), replacement card interception.

Among the most significant frauds can be mentioned:

- 2005-2007 TJX Companies (discount store corporation): computer system intrusion, 45.6 mil. card data sets affected.
- 2008-2009 Heartland (electronic payment processor): computer system intrusion, 130 mil. card data sets affected.
- 2012 Adobe Systems: 40 mil. card data sets.
- 2013 Target Corporation: 40 mil. card data sets.
- 2016 Home Depot: 40 mil. card data sets.

Of course, from a technical point of view, the threat - counter-threat process takes on the dimension of a "technological tango", where each action is followed by a counteraction. So, there are some countermeasures in reaction to these threats:

- Tokenization
- Cardholder supplementary authentication (multi-factor authentication, challenge questions)
- Automated data controls
- Encrypted data

All these countermeasures are included in two of the most important protocols used for securing online card transactions since 1996: SET and 3DS.

2. SET Protocol

Secure Electronic Transaction (SET) is a communication protocol jointly developed by VISA and Mastercard who established in 1996 SET Consortium, with participation of GTE, IBM, Microsoft, Netscape, SAIC, Terisa Systems, RSA, VeriSign. The protocol was designed to address security threats arising to both transmitted and stored data by combining two similar protocols (**Secure Transaction Technology** – from VISA and **Secure Electronic Payment Protocol** - from Mastercard).

SET employs both symmetric and asymmetric cryptography to protect purchasing information sent among SET participants. Key management for SET is based on the use of a Public Key Infrastructure (PKI) to reliably distribute public keys between SET participants [5].

Payment System Participants

- **Cardholder**: in the electronic commerce environment, consumers and corporate purchasers interact with merchants from personal computers. A cardholder uses a payment card that has been issued by an Issuer. SET ensures that in the cardholder's interactions with the merchant, the payment card account information remains confidential.
- **Issuer**: an Issuer is a financial institution that establishes an account for a cardholder and issues the payment card. The Issuer guarantees payment for authorized transactions using the payment card in accordance with payment card brand regulations and local legislation.
- **Merchant**: a merchant offers goods for sale or provides services in exchange for payment. With SET, the merchant can offer its cardholders secure electronic interactions. A merchant that accepts payment cards must have a relationship with an Acquirer.
- **Acquirer**: an Acquirer is the financial institution that establishes an account with a merchant and processes payment card authorizations and payments.
- **Payment Gateway**: a payment gateway is a device operated by an Acquirer or a designated third party that processes merchant payment messages, including payment instructions from cardholders.
- **Certification Authority (CA):** is an entity that is trusted to issue X.509v3 public-key certificates for cardholders, merchants, and payment gateways. The success of SET will depend on the existence of a CA infrastructure available for this purpose. A hierarchy of CAs is used, so that participants need not be directly certified by a root authority [6].

Requirements in SET

- must provide mutual authentication i.e., customer (or cardholder) authentication by confirming if the customer is an intended user or not, and merchant authentication.
- must keep the PI (Payment Information) and OI (Order Information) confidential by appropriate encryptions.
- must be resistive against message modifications i.e., no changes should be allowed in the content being transmitted.
- SET also needs to provide interoperability and make use of the best security mechanisms.

Dual signature

SET introduces a new application of digital signatures, namely the concept of dual signatures. A dual signature is generated by creating the message digest of both messages (payment information and order information), concatenating the two digests together, computing the message digest of the result and encrypting this digest with the signer's private signature key. The signer must include the message digest of the other message for the recipient to verify the dual signature. A recipient of either message can check its authenticity by generating the message digest on its copy of the message, concatenating it with the message digest of the other message (as provided by the sender) and computing the message digest of the result. If the newly generated digest matches the decrypted dual signature, the recipient can trust the authenticity of the message [7].

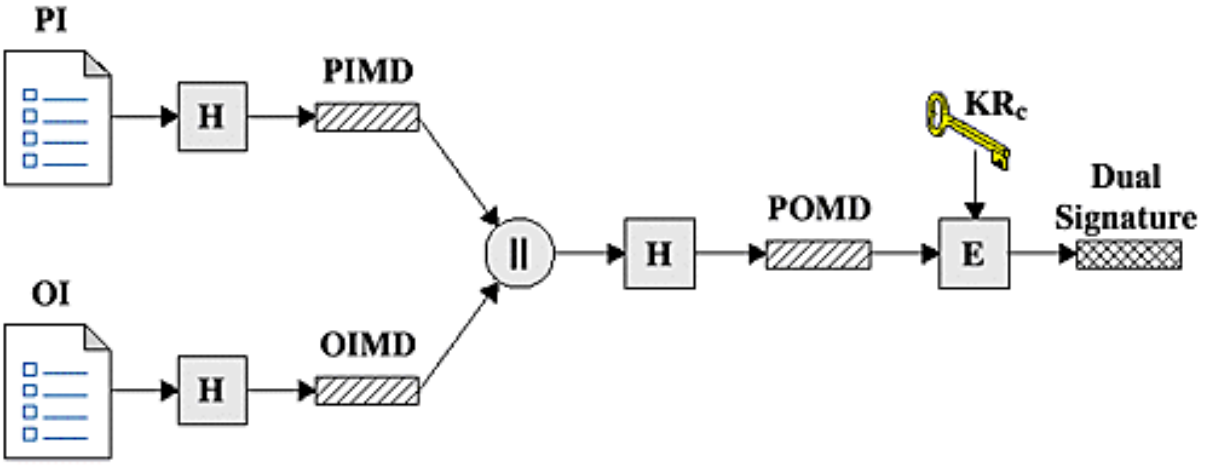


Figure 2.1 Dual signature [6].

Registration and transaction flow [7]

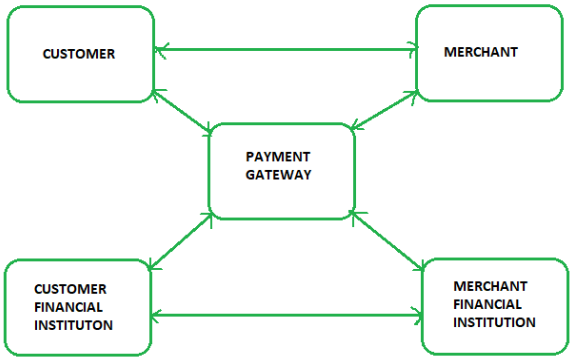


Figure 2.2 SET flow [7].

1. **The customer opens an account.** The customer obtains a credit card account, such as MasterCard or Visa, with a bank that supports electronic payment and SET.
2. **The customer receives a certificate.** After suitable verification of identity, the customer receives an X.509v3 digital certificate, which is signed by the bank. The certificate verifies the customer's RSA public key and its expiration date. It also establishes a relationship, guaranteed by the bank, between the customer's key pair and his or her credit card.
3. **Merchants Have Their Own Certificates.** A merchant who accepts a certain brand of card must be in possession of two certificates for two public keys owned by the merchant: one for signing messages, and one for key exchange. The merchant also needs a copy of the payment gateway's public-key certificate.
4. **The customer places an order.** This is a process that may involve the customer first browsing through the merchant's web site to select items and determine the price. The customer then sends

a list of the items to be purchased from the merchant, who returns an order form containing the list of items, their individual prices, a total price, and an order number.

5. **The merchant is verified.** In addition to the order form, the merchant sends a copy of its certificate, so that the customer can verify that he or she is dealing with a valid store.
6. **The order and payment are sent.** The customer sends both an order and payment information to the merchant, along with the customer's certificate. The order confirms the purchase of the items in the order form. The payment contains credit card details. The payment information is encrypted in such a way that it cannot be read by the merchant. The customer's certificate enables the merchant to verify the customer.
7. **The merchant requests payment authorization.** The merchant sends the payment information to the payment gateway, requesting authorization that the customer's available credit is sufficient for this purchase.
8. **The merchant confirms the order.** The merchant sends confirmation of the order to the customer.
9. **The merchant provides the goods or service.** The merchant ships the goods or provides the service to the customer.
10. **The merchant requests payment.** This request is sent to the payment gateway, which handles all the payment processing.

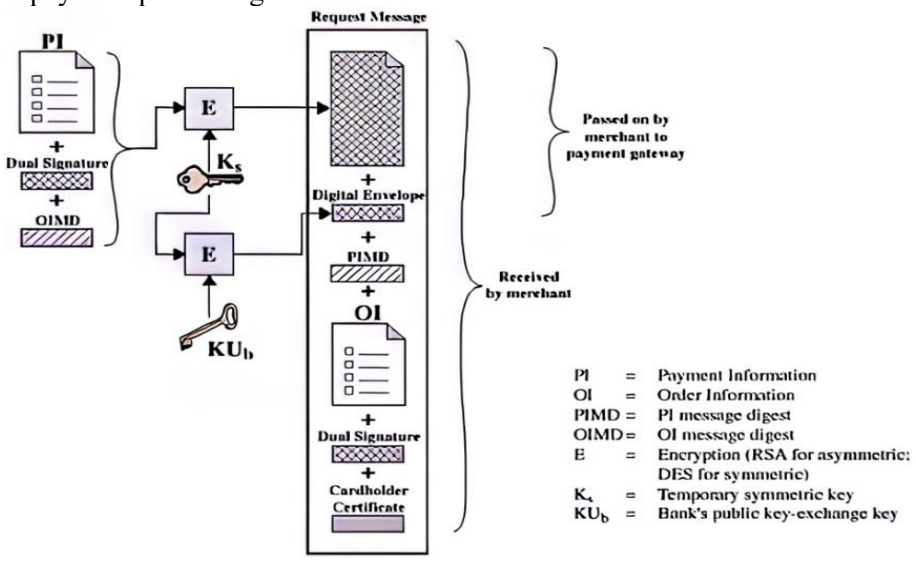


Figure 2.3 Purchase request format [7].

Pro and cons considerations over SET

Pros:

- enhanced security
- global interoperability
- compliance with regulatory standards

Contra:

- complexity of implementation
- limited adoption
- limited industry support
- costly

Arguably, the most secure payment protocol, SET has failed to gain attraction in the market, being phased out by the newer 3d Secure protocol, adopted first by VISA and later, by all major financial services operators.

3. 3D Secure Protocol

Originally developed in 1999 by Celo Communication for Visa Inc., 3D Secure protocol represents a pivotal advancement in online payment security. Initially adopted by VISA as VISA Secure brand, the protocol has also been adopted by Mastercard as Identity Check, by JCB International as JSecure, by American Express as American Express SafeKey and by Discover as ProtectBuy.

In this moment, the protocol is maintained by EMVCo, a consortium created by Visa, Mastercard, JCB, American Express, China UnionPay, and Discover.

3D Secure stands for Three-Domain Secure, and it is a security protocol designed to add an extra layer of authentication for online credit and debit card transactions, the three domains involved in the process being the **acquirer domain, issuer domain** and **interoperability domain** that supports the 3D Secure protocol.

3DS working mode

The 3-D Secure authentication protocol can be:

- **App-based** - Authentication during a transaction on a Consumer Device that originates from an App provided by a registered agent 3DS Requestor (merchant, digital wallet, et al). For example, an e-commerce transaction originating during a check-out process within a merchant's app.
- **Browser-based** - Authentication during a transaction on a Consumer Device that originates from a website utilizing a browser. For example, an e-commerce transaction originating during a check-out process within a website on a Consumer Device.
- **3DS Requestor Initiated** - Confirmation of account information with no direct cardholder present. For example, a subscription-based e-commerce merchant confirming that an account is still valid.

3DS structure and components

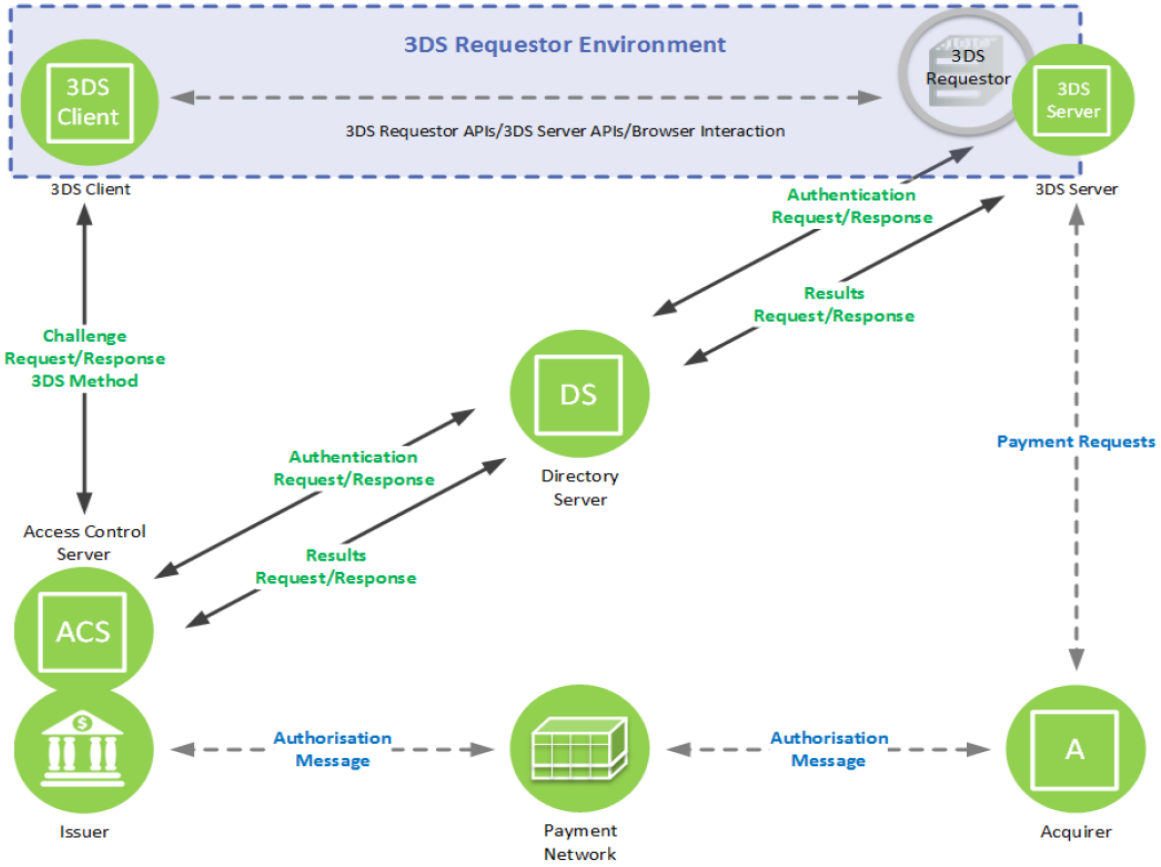


Figure 3.1 3D Secure domain and components [8].

Acquirer domain

- 3DS Requestor Environment
- 3DS Requestor
- 3DS Client
- 3DS Server
- 3DS Integrator
- Acquirer (for Payment Authorization)

Interoperability Domain

- Directory Server (DS)
- Directory Server Certificate Authority (DS CA)
- Authorization System

Issuer Domain

- Cardholder
- Consumer Device
- Issuer
- Access Control Server (ACS)

3DS authentication flow

- Frictionless: for small amounts of money or safe transactions
- Challenge request: meet strong customer authentication (the issuer ask for more information)
- Out of the band: strong customer authentication outside the main communication channel

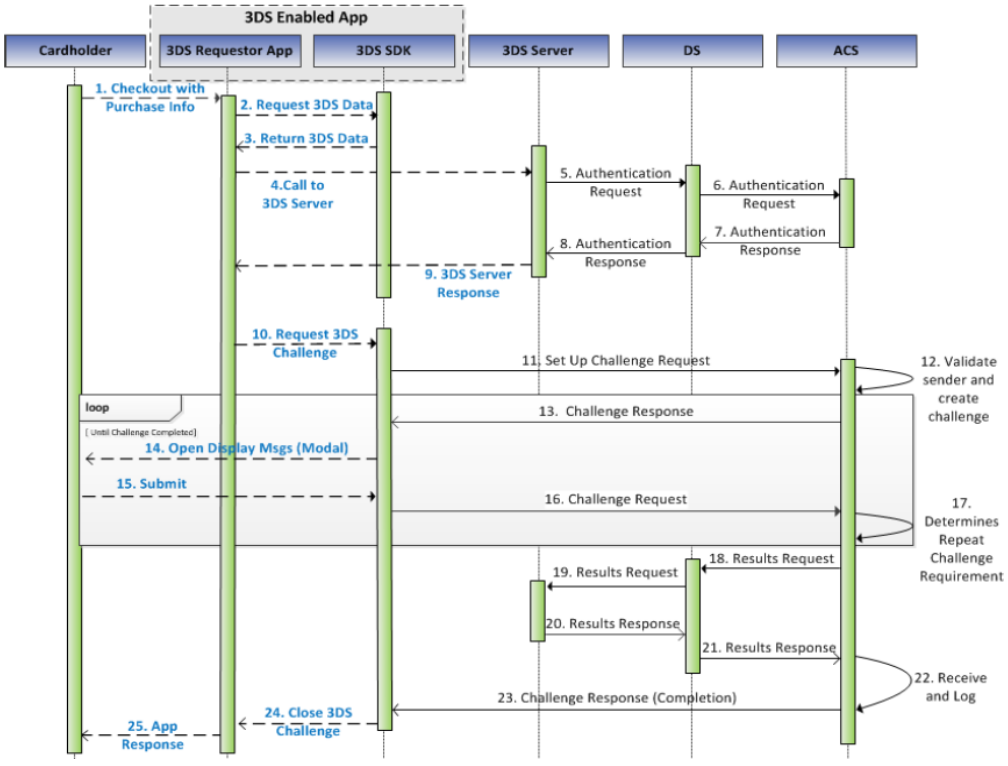


Figure 3.2 Authentication flow [8].

Benefits and limitations

3D Secure v1.0 and lately, v2.0, has emerged with the aim of addressing the drawbacks of its predecessor, the primary benefit of 3DS for merchants being reduced liability of potential chargebacks. If a fraudulent transaction occurs, the card issuer may take responsibility instead of the merchant.

3DS works by authenticating the customer before allowing a transaction, usually involving different methods, like two step authentication, biometric mean, etc. The main downside to 3DS is when it does identify risk with a payment, it creates a lot of friction for customers processing a genuine payment. This causes a decrease in conversion rate and revenue loss which can often be more important than fraud loss itself.

4. Conclusion

Digitization offers enormous opportunities and provides solutions to many of the challenges facing the world, but at the same time it exposes the economy and society to increasingly complex and sophisticated threats, which requires adaptation.

Specific domain, payment security refers to the technologies, processes, and measures employed to protect financial transactions from unauthorized access, data breaches, and fraud. This builds confidence in payment systems, ensuring adherence to legal and regulatory requirements.

First widely accepted payment security protocol, SET was a major achievement in this area. Offering advanced security, it was arguably the most secure protocol. Enthusiastic supported at the beginning, this was waned in time because of complex procedures and implementation, association with the Public Key Infrastructure (complicated initialization and registration), hardware dependence, etc.

3D Secure has emerged as a more flexible arrangement designed to protect the online payment flows. When launched at the beginning of 2000`s as 3D Secure v.1, computers were the only available devices for online shopping, so, naturally, this version was optimized for desktop authentication, as long mobile smartphones were not available. Lately, with the advance of mobile telecommunications technologies, this rigidity together with necessity of some static passwords, determined friction and extra operational costs.

When released in 2016, 3D Secure v.2 managed to address some of the old's protocol pain points, bringing increased protection, minimizing frictions and improving chargeback management.

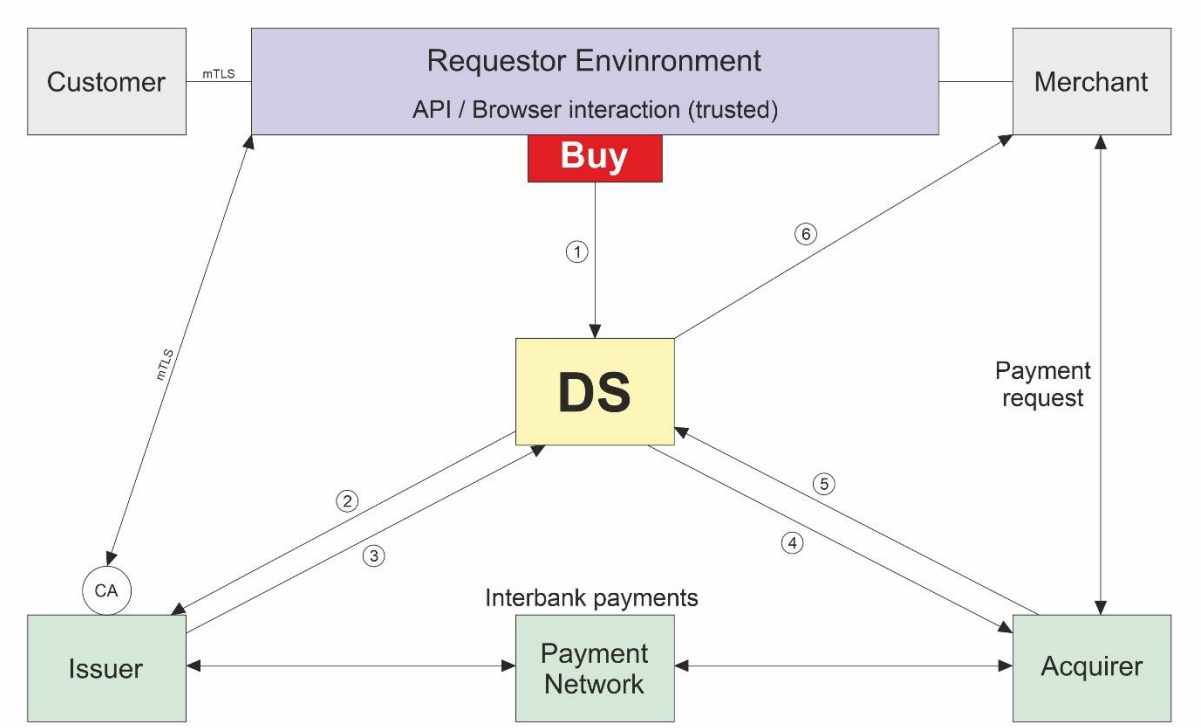
In this time, banking card fraud across the world steadily increased, peaking at the end of 2022 a staggering amount of 30 billion USD – 12 billion USD coming from USA [9].

Regarding this, further development of protocols must be closely linked to developments in the cyber area, both by monitoring trends in services and possible threats emerging in parallel with newly developed services.

From a systems security point of view, several trends can be noted [10]:

- zero-trust cybersecurity model - nothing is left to chance, no system is assumed to be secure, which is why it is constantly tested to identify and eliminate vulnerabilities, no matter how little exposed it may seem at first glance.
- passwordless authentication - industry-wide changes towards widespread adoption of passwordless authentication are expected in the near future. Traditional written password protection will be replaced by other means such as multi-factor authentication, mobile codes, or biometrics.
- artificial intelligence-based security - artificial intelligence will play an increasingly important role in cyber threat detection, automated responses and protection protocols. Using autonomous systems for these aspects of security management is highly efficient and timesaving.

Based on the advantages of both protocols and the trends in computer security, some new protocols can be created, like the one bellow:



Prerequisite:

- Issuer, Acquirer are Private Certification Authority
- Customer and Merchant obtain x.509 certificate at the time of enrolment (Private PKI)
- All the connections are mTLS based.

Flow:

1. After the Customer finishes the process of buying, Requestor forward to DS participant's ID, together with transaction ID and total amount.
2. DS request Issuer authorization, sending Customer ID, Transaction ID and total amount.
3. Issuer sends an authorization token to DS (Customer ID, Transaction ID, IssAuthID).
4. DS sends an authorization token to Acquirer (Merchant ID, Transaction ID, IssAuthID).
5. Acquirer sends an authorization response (Merchant ID, Transaction ID, AcqAuthID).
6. DS sends a transaction authorization (Transaction ID, IssAuthID, AcqAuthID).

All the payment requests are further based on the Transaction ID, IssAuthID, AcqAuthID.

The scheme presented above uses the specific 3D Secure structure over the public key authentication procedures used by SET. This technical approach has several advantages:

- is compliant with the trends in cyber security: passwordless authentication, zero-trust security.
- reduces the numbers of network nodes.
- is compliant with the concept "need to know", each participant receiving only the necessary information to decide.
- using a private Public Key Infrastructure and x.509 certificates, a strong authentication is achieved eliminating the need to use financial information such as bank card or account details.

5. References

[1] Politechnical University of Timișoara – "IT Platforms For Production and Services.06 Electronic commerce" - course support, https://www.aut.upt.ro/staff/diercan/data/PIPPS/curs-06.pdf

[2] European Central Bank – Press release, 9 September 2023 https://www.ecb.europa.eu/press/stats/paysec/html/ecb.pis2022~8bb6cc08f4.en.html

[3] STATISTA Corporation - https://www.statista.com/statistics/1394119/global-card-fraud-losses/#statisticContainer

[4] Clearly Payments - https://www.clearlypayments.com/blog/credit-card-fraud-in-2023/

[5] Chris J. Mitchell – "Implementation Aspects of SET/EMV", Conference paper - 2002, DOI: 10.1007/978-0-387-35617-4_20, https://www.researchgate.net/publication/220895745

[6] William Stallings - Introduction to Secure Electronic Transaction (SET), 17 May 2002, InformIT by Pearson Media (https://www.informit.com/articles/article.aspx?p=26857)

[7] SET LLC (SETco) - Secure Electronic Transaction Specification, Book1: Business Description

[8] EMV LLC (EMVco) – 3D Secure: Protocol and Core Functions Specification v2.2.0 - 2018

[9] STATISTA Corporation - https://www.statista.com/statistics/1394119/global-card-fraud-losses/

[10] Nicolae Nebancea, Ciprian Răcuciu – "TRENDS IN THE SECURITY OF THE MOBILE AND WIRELESS NETWORK AND THE NEW EMERGENT RISKS", Titu Maiorescu University - International Conference, November 2023