



Automated Security and Risk Analysis of Strong Customer Authentication Solutions for the PSD2

Marco Pernpruner

Security & Trust Research Unit
Fondazione Bruno Kessler, Trento, Italy

Recent Security Advances in the Finance Sector
January 14, 2021

| Agenda

- Overview of Security Vulnerabilities Affecting the Financial Scenario
- Payment Services Directive 2 (PSD2)
- Automated Analysis of Security Protocols for the PSD2



| Agenda

- **Overview of Security Vulnerabilities Affecting the Financial Scenario**
- Payment Services Directive 2 (PSD2)
- Automated Analysis of Security Protocols for the PSD2



| Security Vulnerabilities

Android malware can steal Google Authenticator app

A new version of the "Google Authenticator" app and

Cerberus banking Trojan source code released for free to cyberattackers

An auction designed to net the developer of the Android malware \$100,000 failed.

TrickMo

bypassing 2FA

Lock

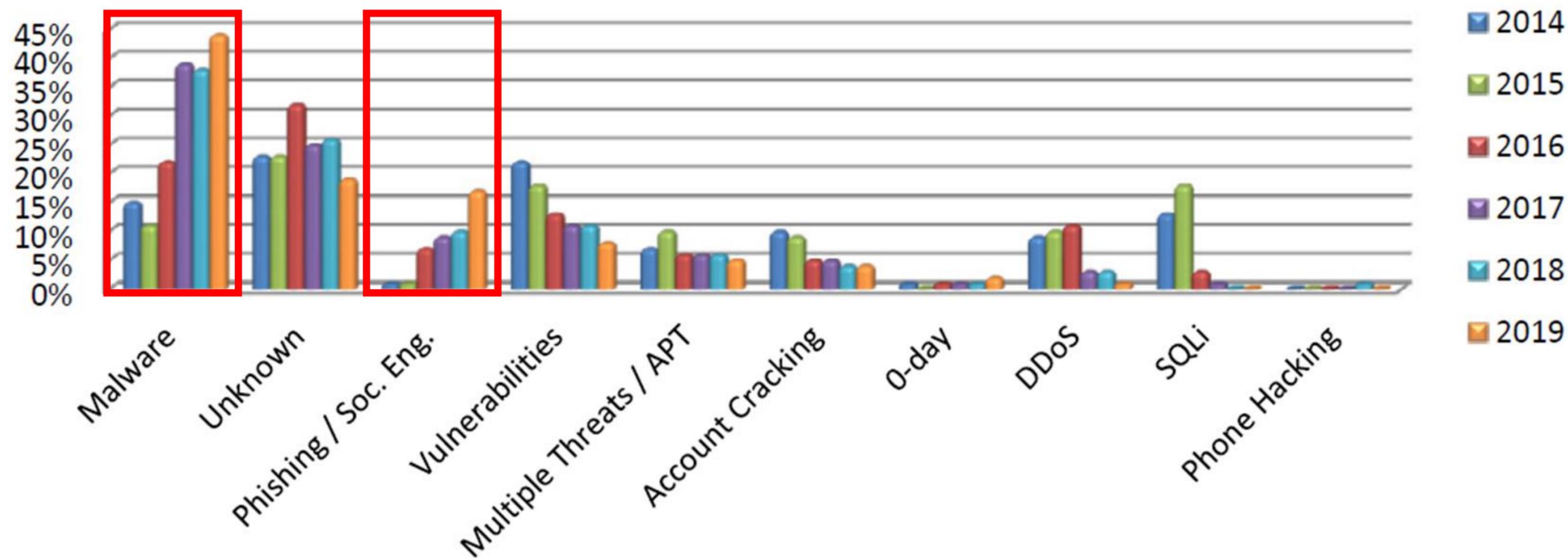
Malicious TrickMo app seen deployed in Germany for now, but broader use is

New 'Alien' malware can steal passwords from 226 Android apps

Most targets are banking apps, but Alien can also show phishing pages for social, instant messaging, and cryptocurrency apps.

passwords and two-factor codes

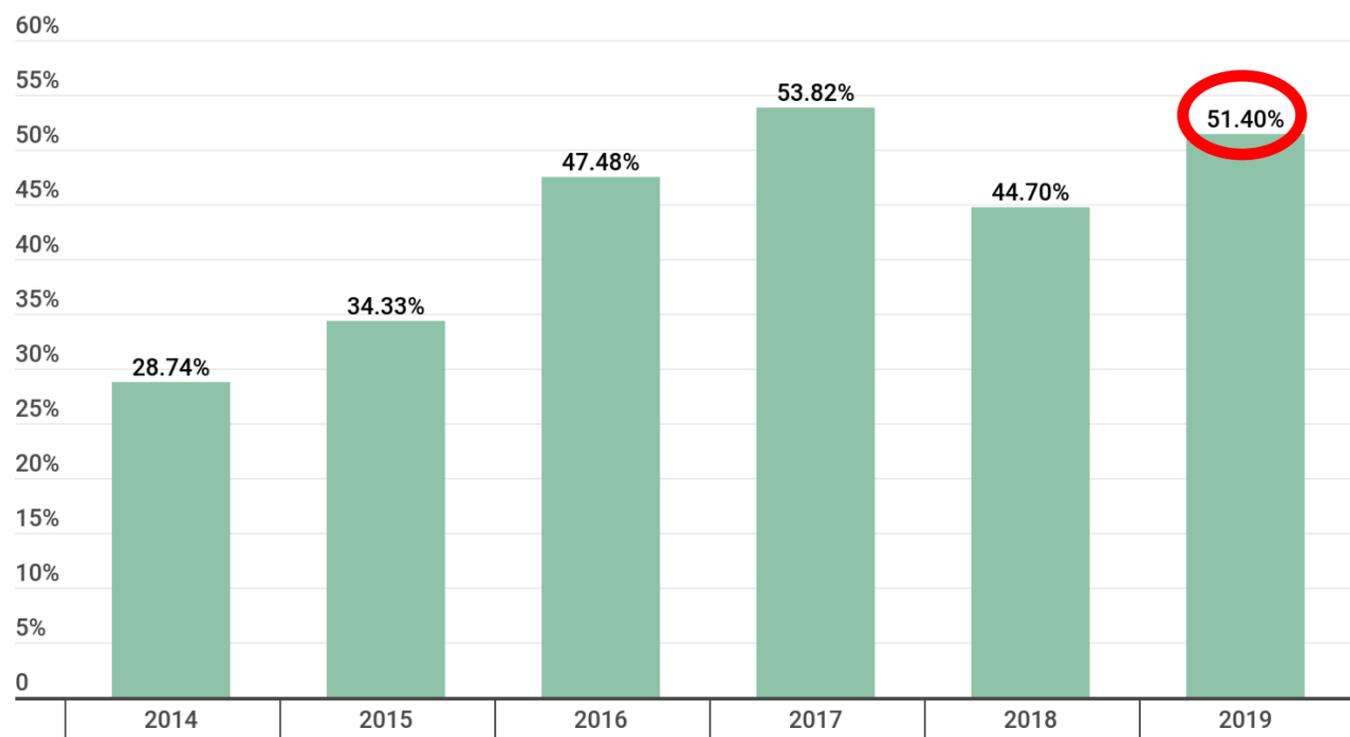
Security Vulnerabilities Techniques



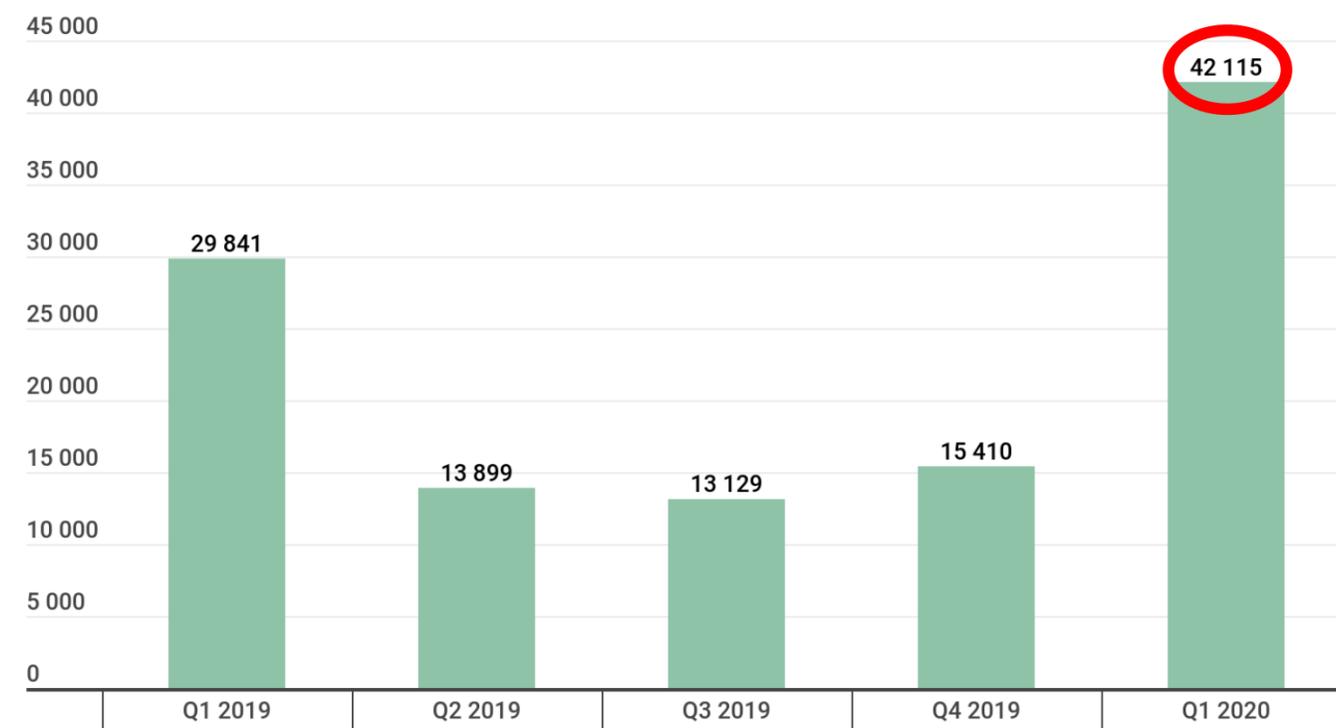
© Clusit - Rapporto 2020 sulla Sicurezza ICT in Italia

Security Vulnerabilities

Financial Phishing and Malware



The percentage of financial phishing attacks (from overall phishing attacks) detected by Kaspersky, 2014-2019



Number of installation packages of mobile banking trojans detected by Kaspersky, Q1 2019 – Q1 2020

Security Vulnerabilities

Skimming

General

Request URL: `https://myicons.net/d/favicon.png`

Request Method: GET

Status Code: 200 OK

Remote Address: [REDACTED]

Referrer Policy: no-referrer-when-downgrade

Response Headers

Connection: Keep-Alive

Content-Length: 6251

Content-Type: `image/png`

Date: [REDACTED]

Keep-Alive: timeout=5, max=100

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.4.16

X-Powered-By: PHP/5.4.16

Request Headers

Accept: */*

Accept-Encoding: gzip, deflate, br

Accept-Language: en-US,en;q=0.9

Connection: keep-alive

Host: myicons.net

Referer: `https://www.[REDACTED].html`



PNG

General

Request URL: `https://myicons.net/d/favicon.png`

Request Method: GET

Status Code: 200 OK

Remote Address: [REDACTED]

Referrer Policy: no-referrer-when-downgrade

Response Headers

Connection: Keep-Alive

Content-Length: 14885

Content-Type: `text/html`

Date: [REDACTED]

Keep-Alive: timeout=5, max=100

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2

Set-Cookie: `pxcelPage_c01003=https%3A%2F%2Fwww.[REDACTED]`

X-Powered-By: PHP/5.4.16

Request Headers

Accept: */*

Accept-Encoding: gzip, deflate, br

Accept-Language: en-US,en;q=0.9

Connection: keep-alive

Host: myicons.net

Referer: `https://www.[REDACTED]/checkout/`

Preview

Credit Card

Credit Card Type *

--Please Select--

Credit Card Number *

Name on Card *

Expiration Date *

January 2020

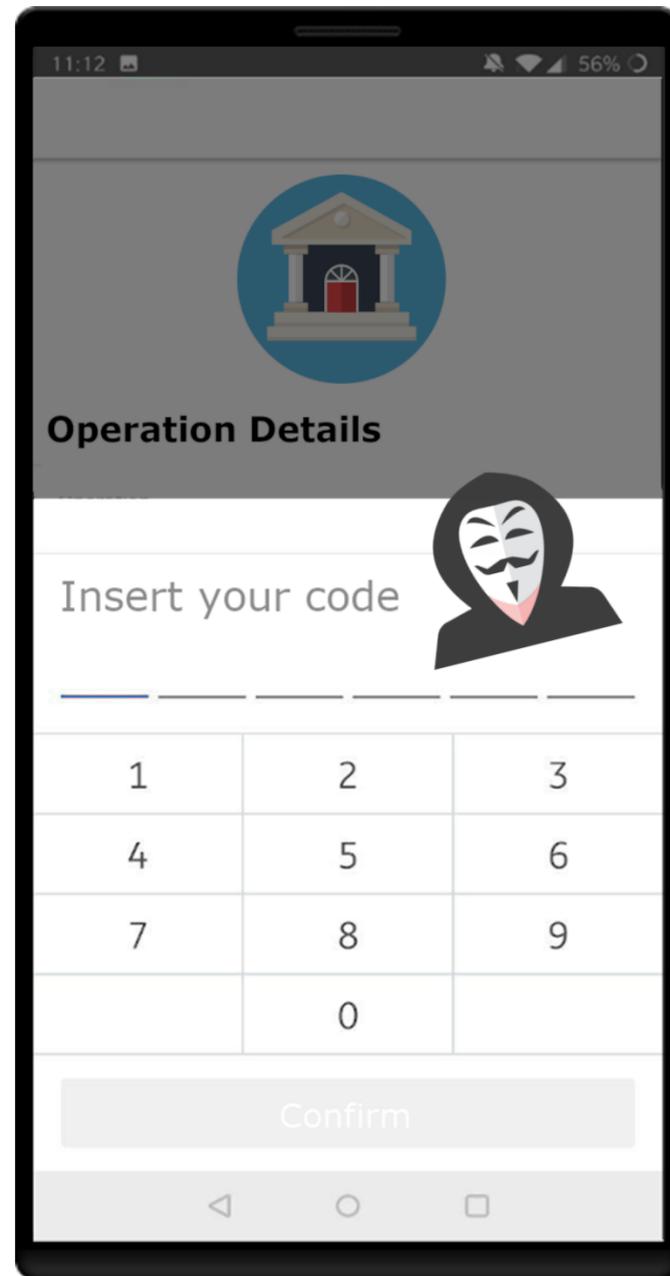
Card Verification Number *



HTML

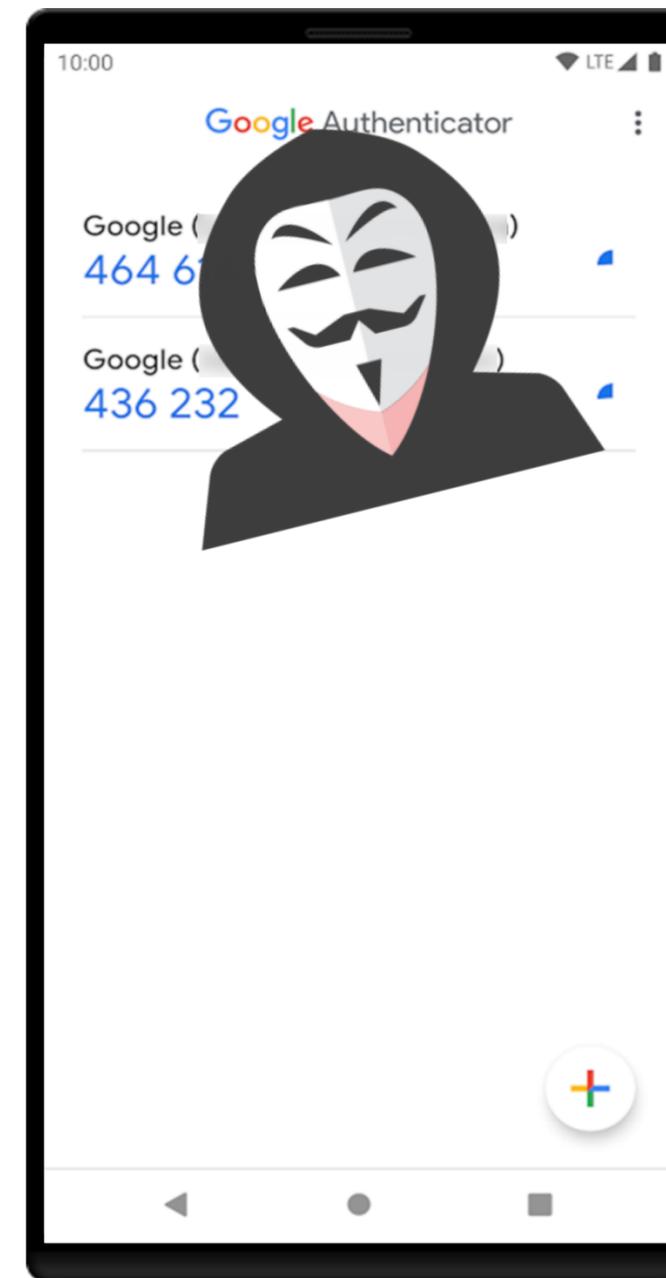
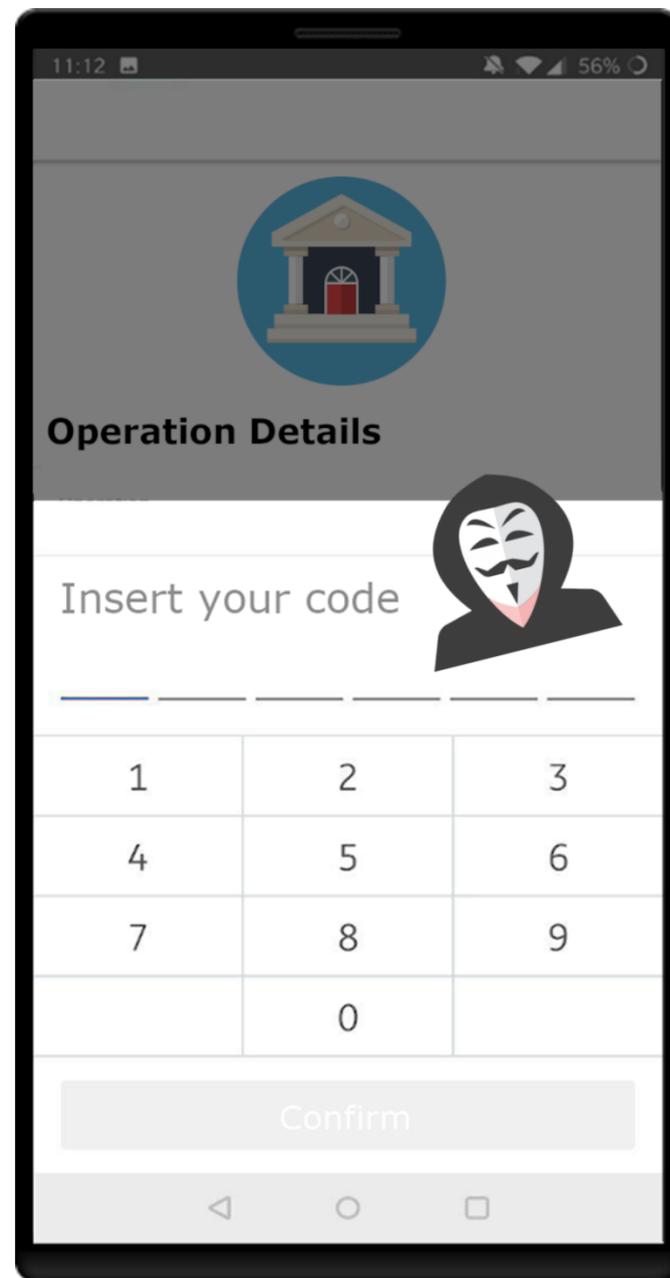
Security Vulnerabilities

TrickBot



Security Vulnerabilities

TrickBot



| Agenda

- Overview of Security Vulnerabilities Affecting the Financial Scenario
- **Payment Services Directive 2 (PSD2)**
- Automated Analysis of Security Protocols for the PSD2



| Payment Services Directive (PSD2)



Directive (EU) 2015/2366 regarding payment services in the internal market.



Open Banking

Fostering the birth of new innovative solutions built around financial institutions



Security

Improving the security of e-banking protocols

Payment Services Directive (PSD2)

Directive (EU) 2015/2366 regarding payment service



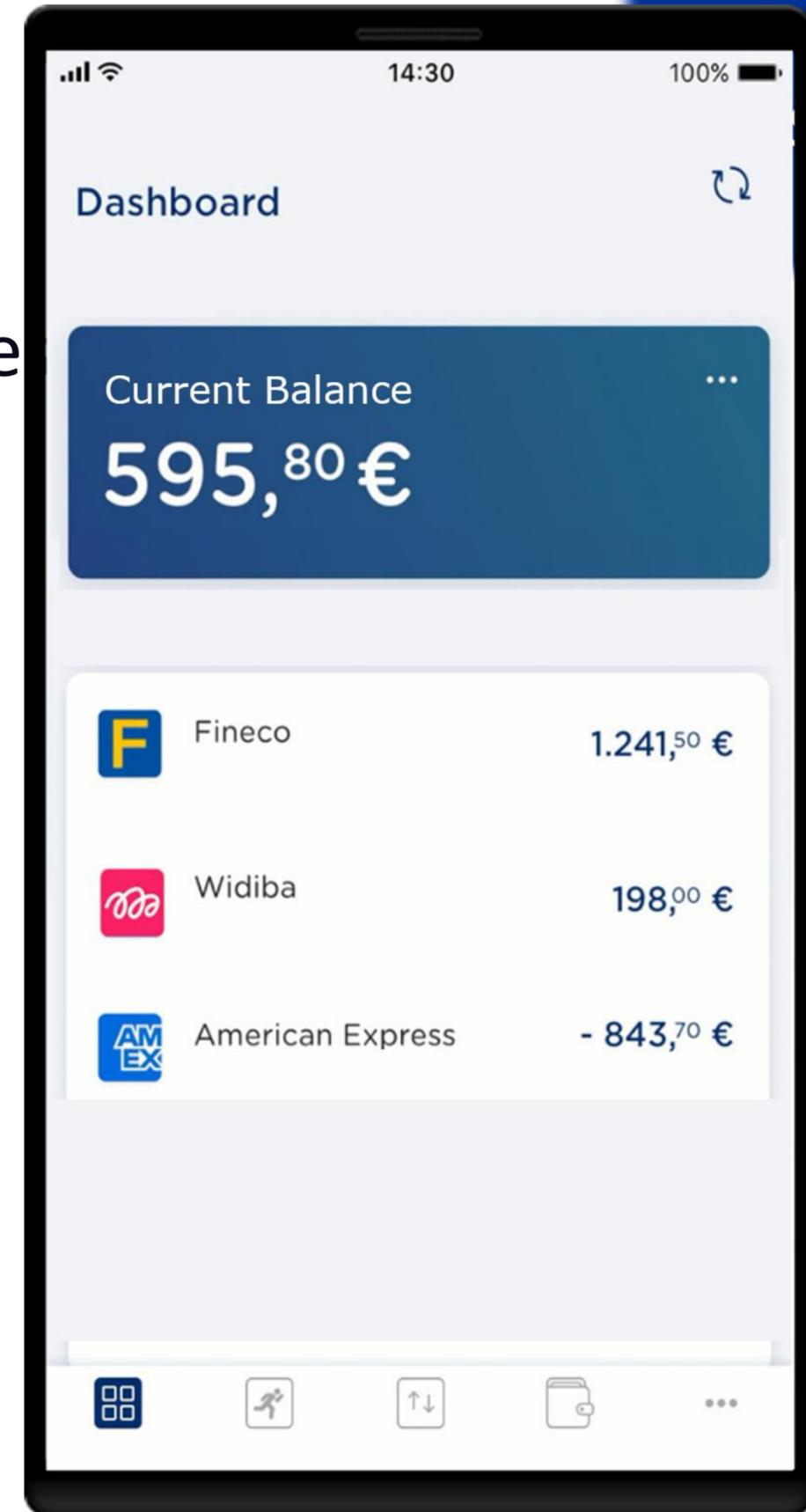
Open Banking

Fostering the birth of new innovative solutions built around financial institutions



Security

Improving the security of e-banking protocols



| Payment Services Directive (PSD2)



Directive (EU) 2015/2366 regarding payment services in the internal market.



Open Banking

Fostering the birth of new innovative solutions built around financial institutions



Strong Customer Authentication (SCA)



Security

Improving the security of e-banking protocols



Dynamic Linking

Payment Services Directive (PSD2)

Strong Customer Authentication (SCA)

Authentication relying on more than a single *authentication factor*:



Actions	SCA required?
Balance inquiry	Depends on the case
Consultation of payment history of past 90 days	Depends on the case
Payments to trusted beneficiaries	Depends on the case
Recurrent payments with same amount and same payee	Depends on the case
Payments not exceeding € 30	Depends on the case
Payments exceeding € 30	Always

Payment Services Directive (PSD2)

Dynamic Linking

During a transaction, the *authentication code* must be strongly connected with the ongoing operation.

Transfer no.	AA/1234
Payer Name	John Smith
Payee Name	Anne Smith
Payee IBAN Code	IT12T1234512345123456789012
Amount	100,00 EUR



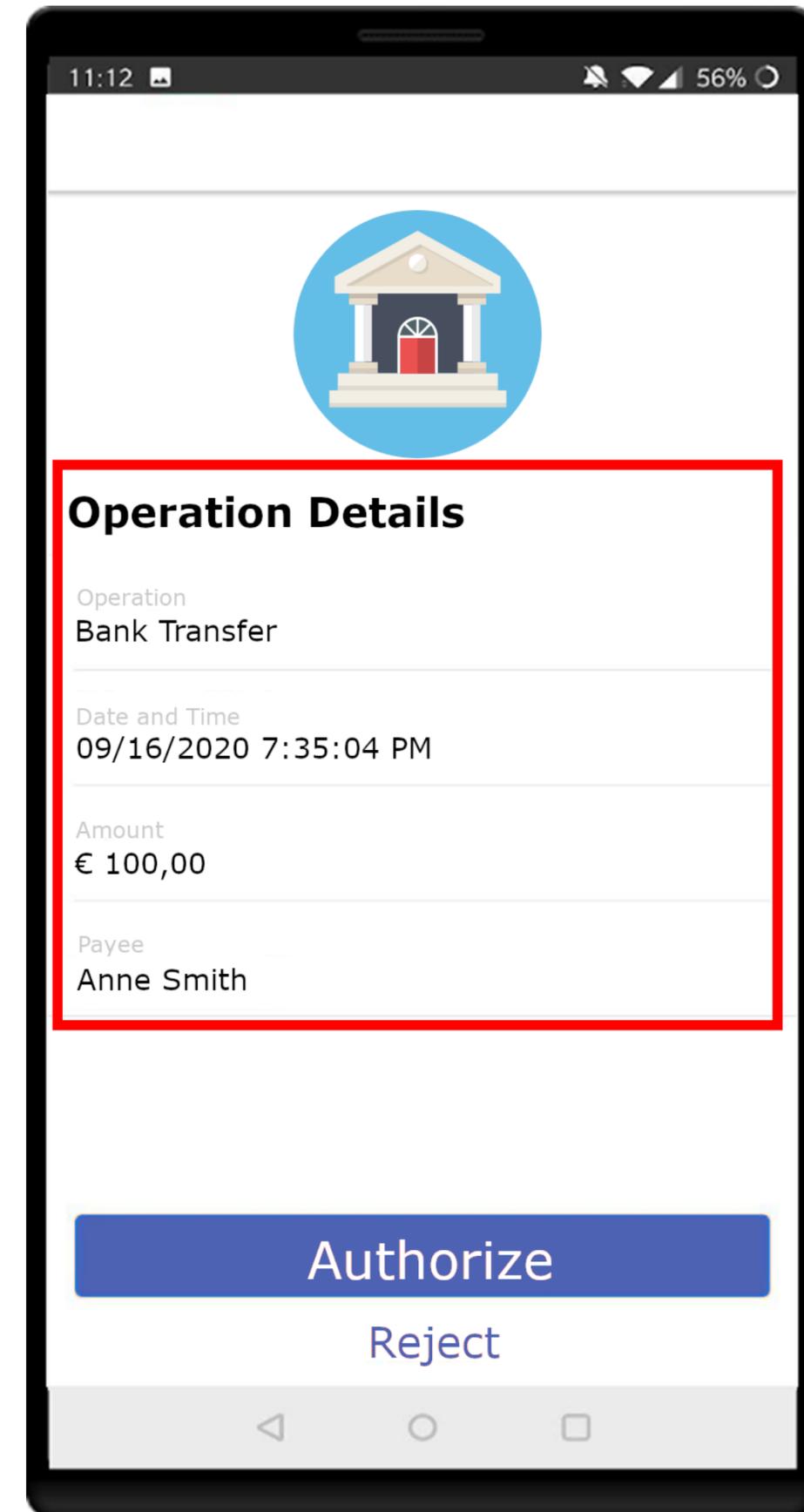
authentication code



Payment Services Directive (PSD2)

Dynamic Linking

Moreover, the user is always displayed the operations' details before the authorization.



Use Case Before PSD2

Before
PSD2

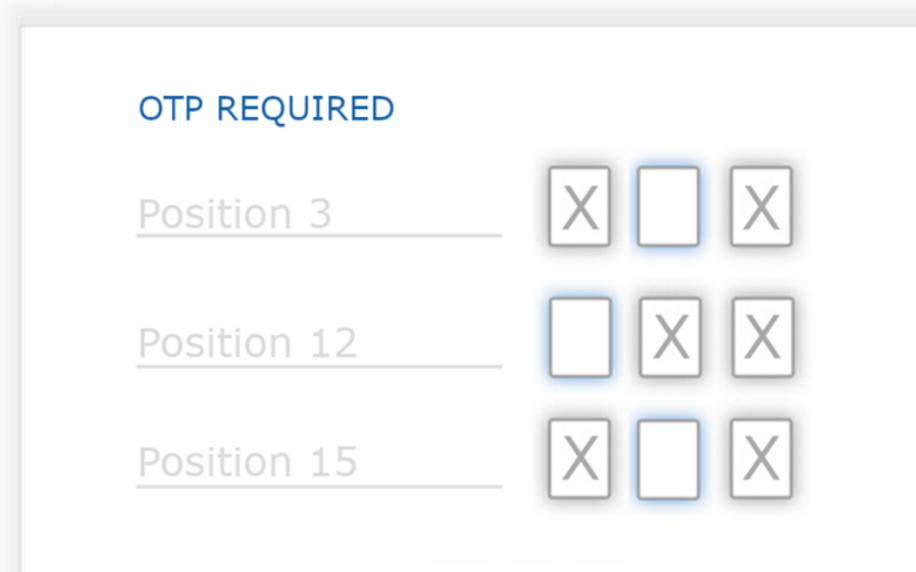
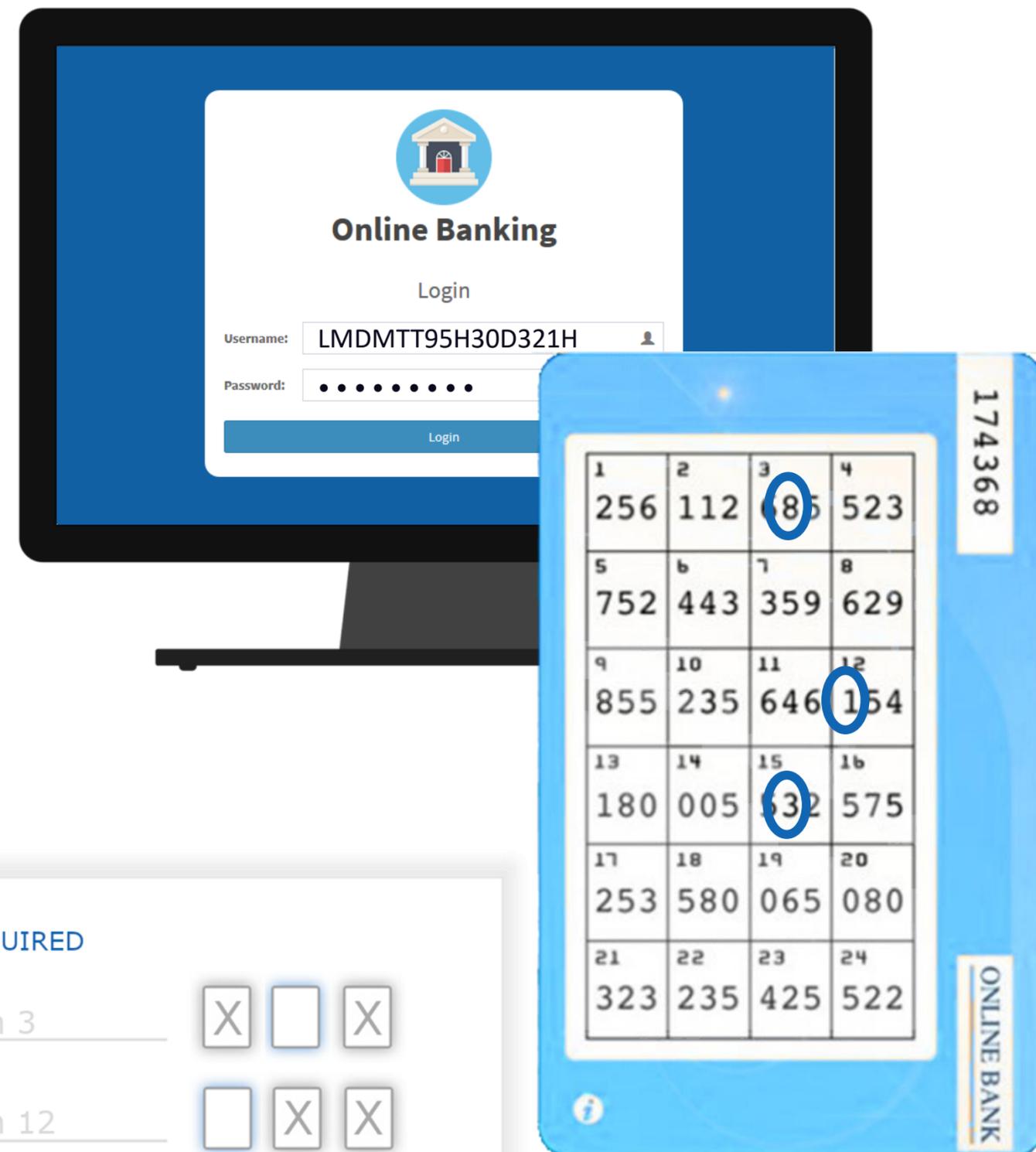
1. The user authenticates on the online banking through credentials and performs an operation.



Use Case Before PSD2

Before
PSD2

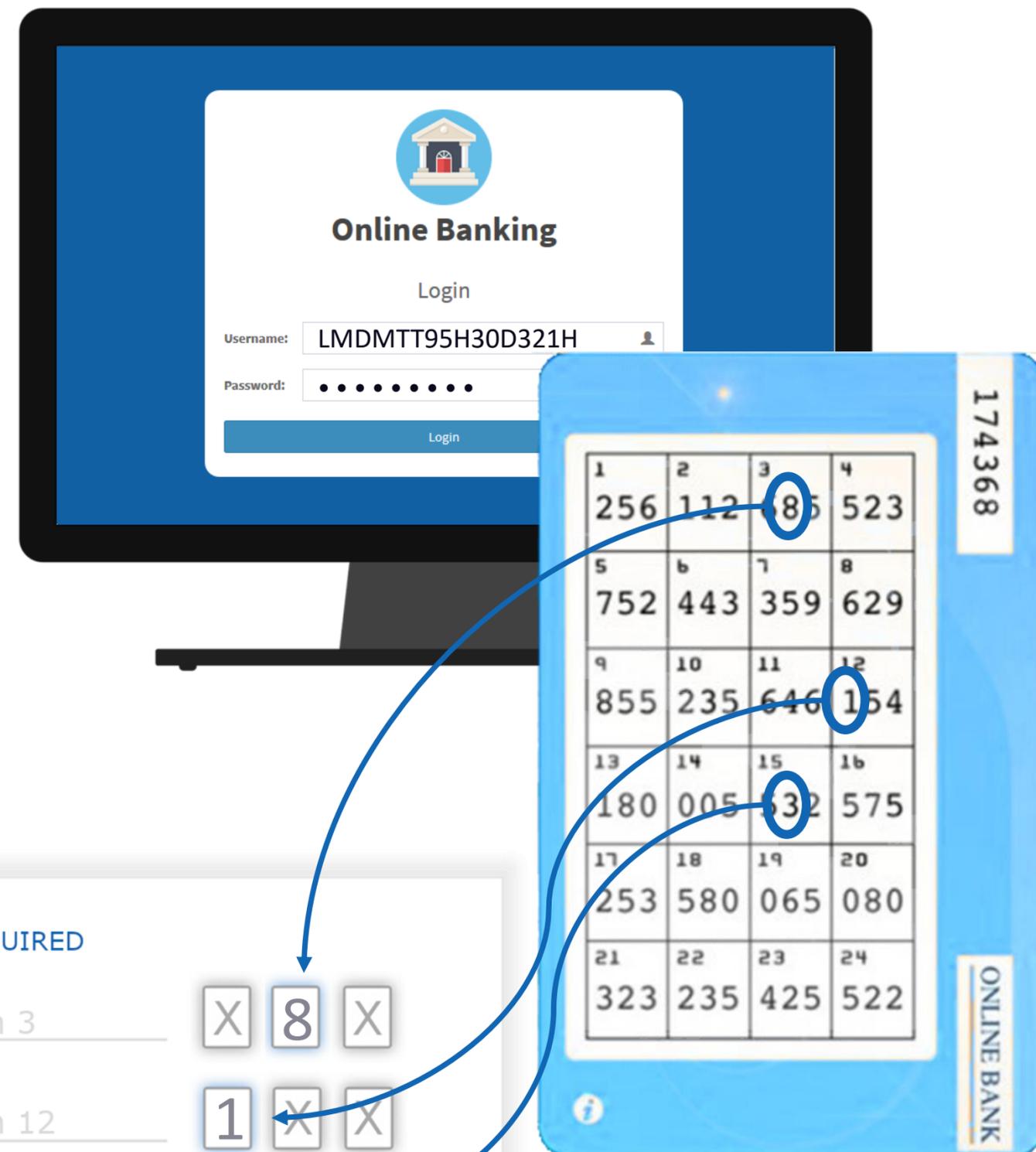
1. The user authenticates on the online banking through credentials and performs an operation.
2. The user generates a code through the matrix.



Use Case Before PSD2

Before
PSD2

1. The user authenticates on the online banking through credentials and performs an operation.
2. The user generates a code through the matrix.
3. The user inserts the code in the online page to authorize the operation.

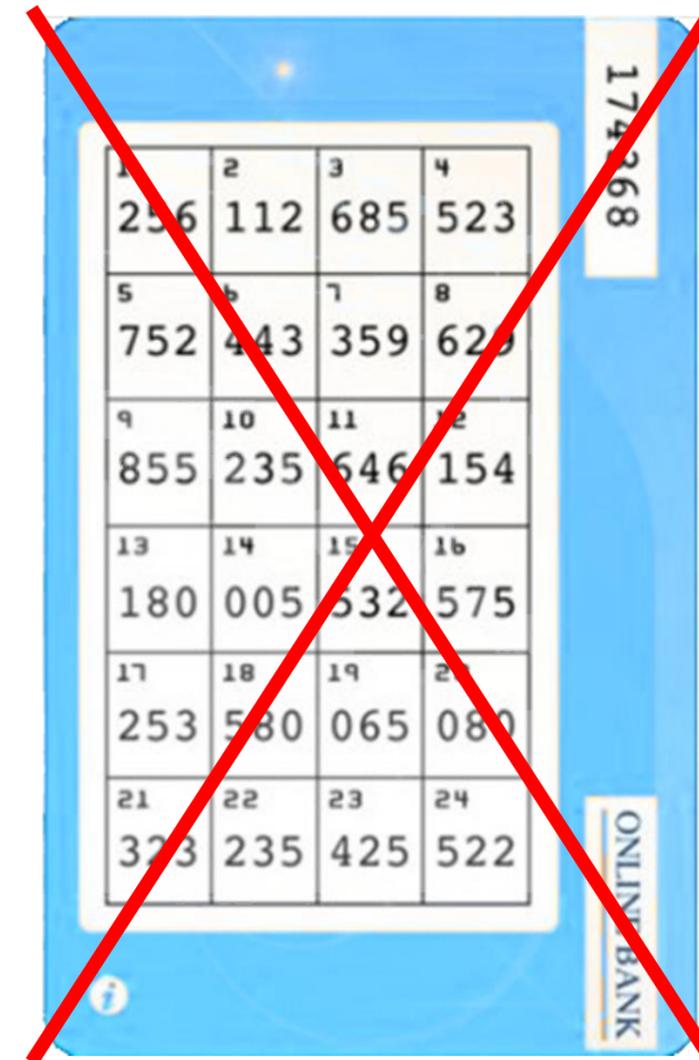


Payment Services Directive (PSD2) Not Compliant Solutions

1. The authentication code is not connected with the ongoing operation.



2. Users cannot be aware of which operation they are about to authorize.



Use Case After PSD2

After
PSD2

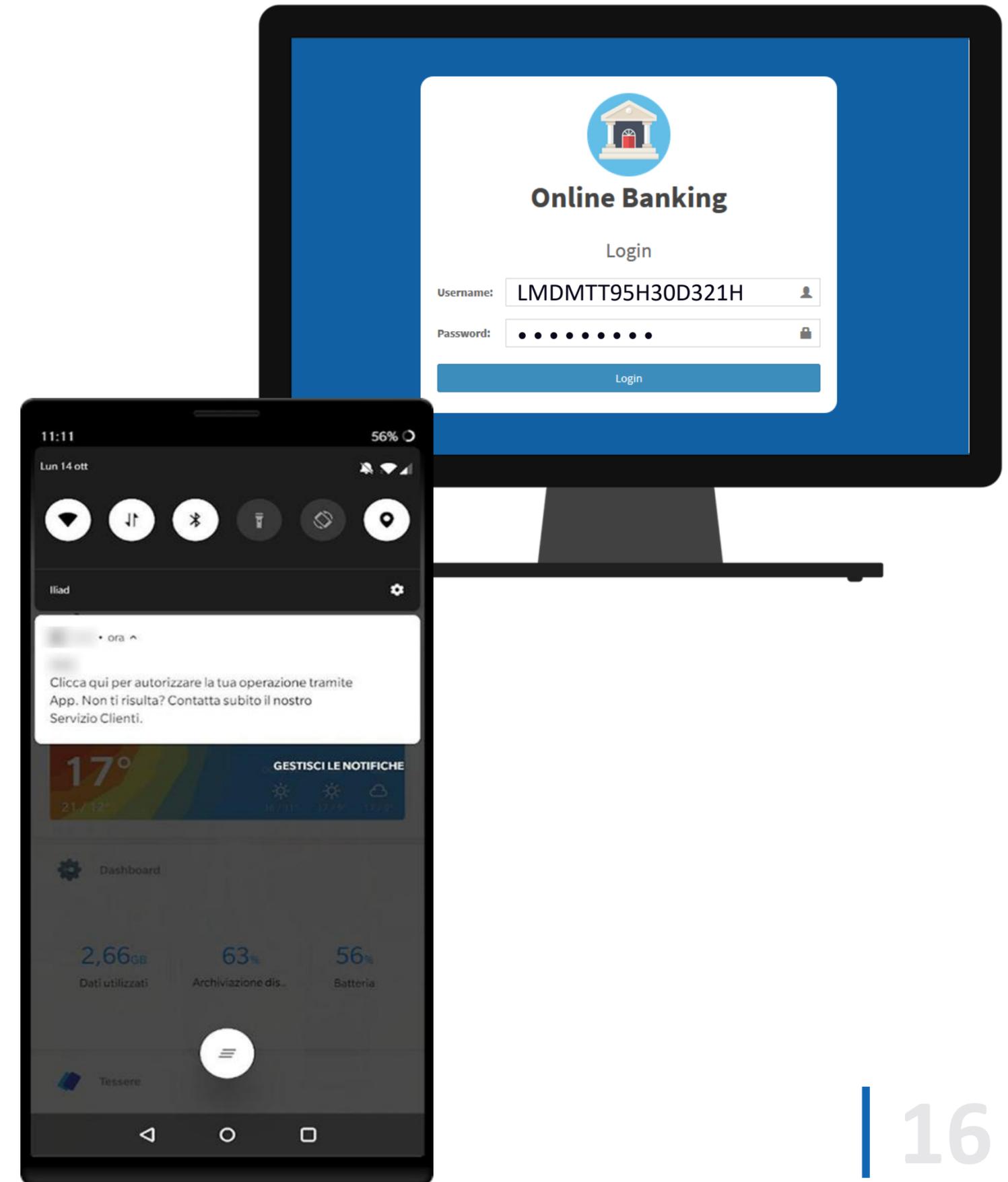
1. The user authenticates on the online banking through credentials and performs an operation.



Use Case After PSD2

After
PSD2

1. The user authenticates on the online banking through credentials and performs an operation.
2. The user receives a *push notification* that, once opened, details the ongoing operation.



Use Case After PSD2

After
PSD2

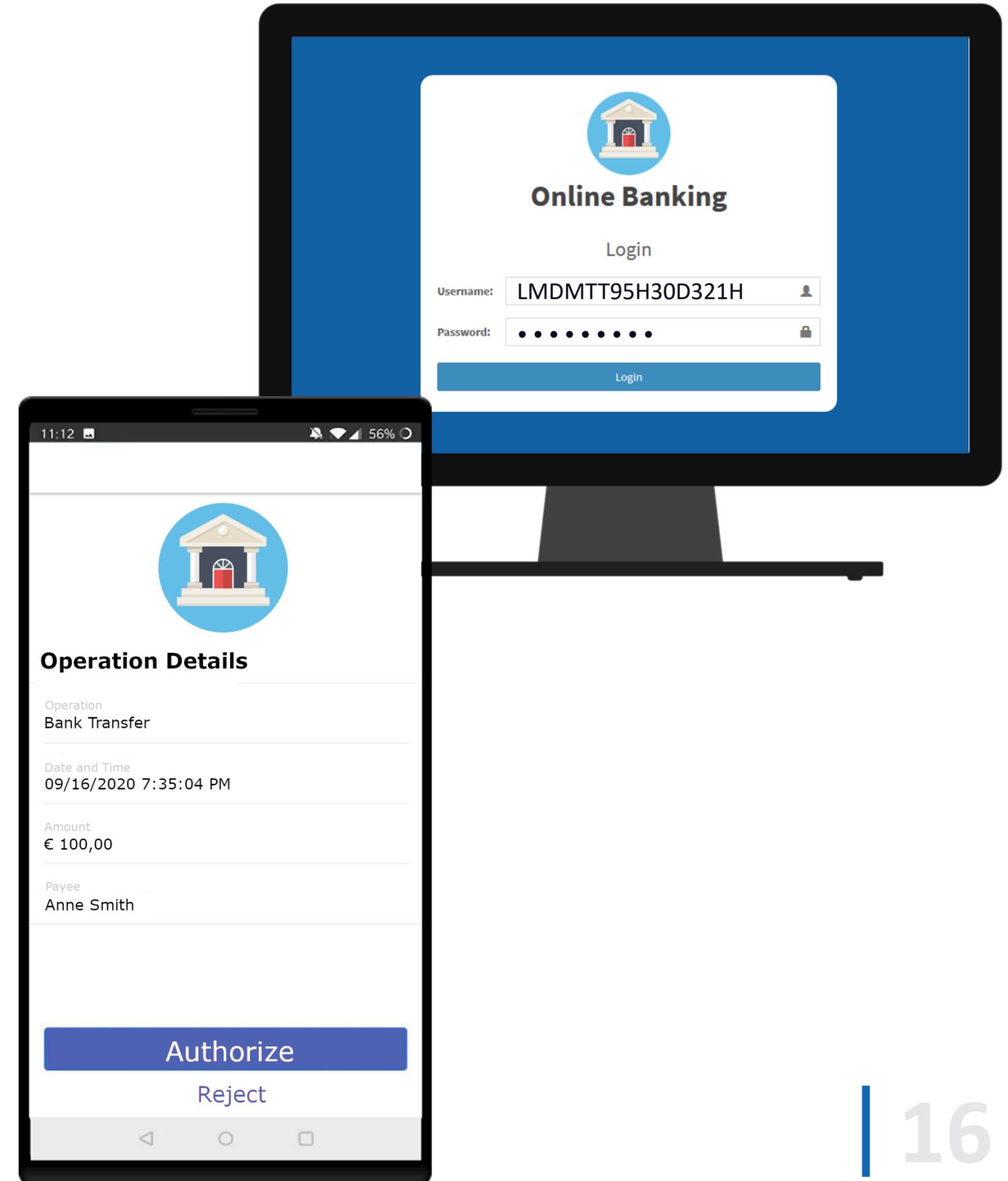
1. The user authenticates on the online banking through credentials and performs an operation.
2. The user receives a *push notification* that, once opened, details the ongoing operation.



Use Case After PSD2

After
PSD2

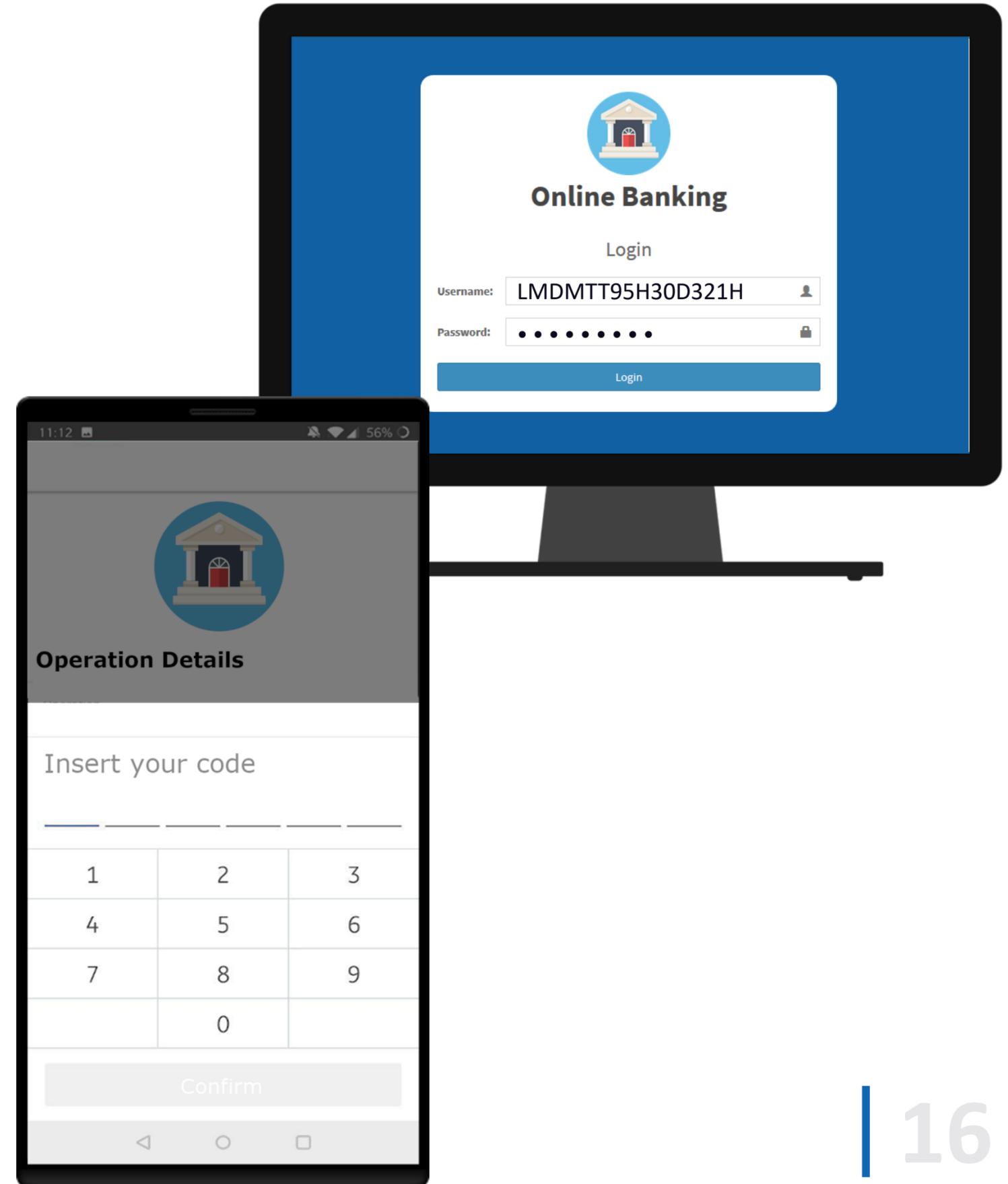
1. The user authenticates on the online banking through credentials and performs an operation.
2. The user receives a *push notification* that, once opened, details the ongoing operation.



Use Case After PSD2

After
PSD2

1. The user authenticates on the online banking through credentials and performs an operation.
2. The user receives a *push notification* that, once opened, details the ongoing operation.
3. By inserting a specific PIN, the user can authorize the operation.



Use Case

Compliance with the PSD2

Requirement	Before PSD2	After PSD2
Strong Customer Authentication	 Factors: credentials (K) matrix (P)	 Factors: credentials (K) smartphone (P)
Dynamic Linking (link between authentication code and operation)	 Matrices cannot generate codes linked to the ongoing operation	 Authentication code is bound to the ongoing operation
Dynamic Linking (information on the operation displayed to the user)	 Matrices cannot display any information about the ongoing operation	 Details on the ongoing operation are displayed after clicking on the notification

| Agenda

- Overview of Security Vulnerabilities Affecting the Financial Scenario
- Payment Services Directive 2 (PSD2)
- **Automated Analysis of Security Protocols for the PSD2**



Automated Analysis of Security Protocols for the PSD2

A Two-Levels Approach

1

Security Analysis

To detect the attackers that manage to compromise the protocol

2

Risk Analysis

To evaluate the risks connected with the successful attackers detected

Automated Analysis of Security Protocols for the PSD2

A Two-Levels Approach

1

Security Analysis

To detect the attackers that manage to compromise the protocol

2

Risk Analysis

To evaluate the risks connected with the successful attackers detected

Automated Analysis of Security Protocols for the PSD2

Security Analysis

To detect the attackers that manage to compromise the protocol, we perform two different kinds of analysis:

1. **Combinatorial Analysis:** relying on attackers' capabilities on the authentication factors. It is fast and thus helps prune the set of attackers to test, but may not detect some advanced attacks.
2. **Formal Analysis:** relying on formal methods (a specification language and a model checker). It can be computationally expensive, but manages to find even more complex categories of attacks.

Automated Analysis of Security Protocols for the PSD2

Security Analysis

To detect the attackers that manage to compromise the protocol, we perform two different kinds of analysis:

1. **Combinatorial Analysis:** relying on attackers' capabilities on the authentication factors. It is fast and thus helps prune the set of attackers to test, but may not detect some advanced attacks.
2. **Formal Analysis:** relying on formal methods (a specification language and a model checker). It can be computationally expensive, but manages to find even more complex categories of attacks.

Automated Analysis of Security Protocols for the PSD2

MuFASA



Secret
Device
App

Authentication factors

It requires a secret code (e.g., a PIN)? yes ▼

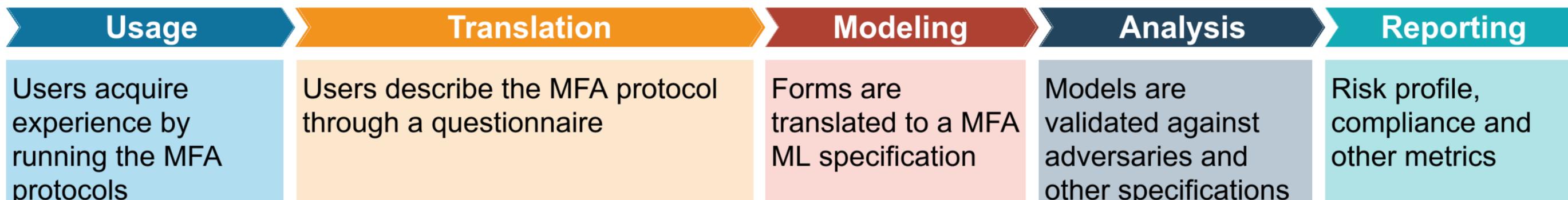
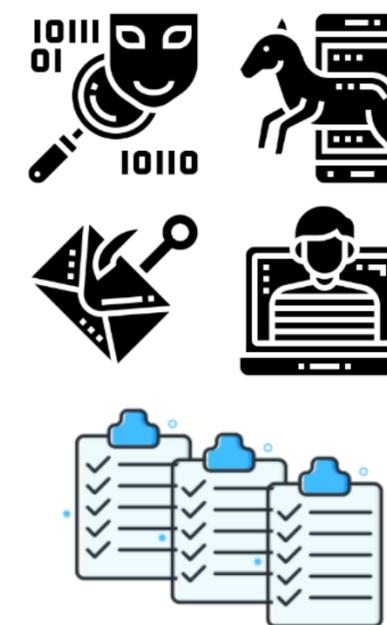
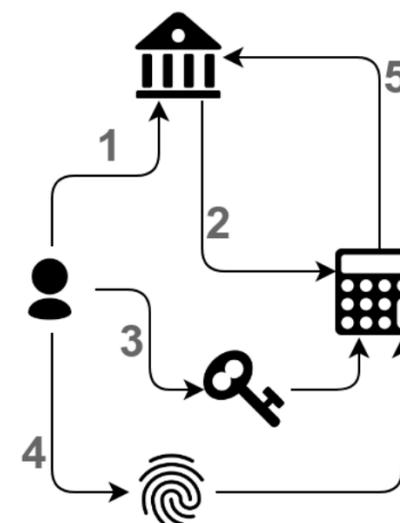
It requires a biometric scan (e.g., fingerprints)? no ▼

It requires an object you own (e.g., a smart card)? yes ▼

Input/output

I have to manually input a code yes ▼

I receive the code via sms ▼



Automated Analysis of Security Protocols for the PSD2



MuFASA – Translation



From which endpoint do you start the protocol?

I start the protocol from a desktop computer

I start the protocol from my smartphone

What kind of data does your service process?

anonymous data

personal data

sensitive data

financial data

[Previous](#) [Next](#)

Automated Analysis of Security Protocols for the PSD2



MuFASA – Translation



Endpoint: Desktop

Protocol specified so far:

What is your next operation?

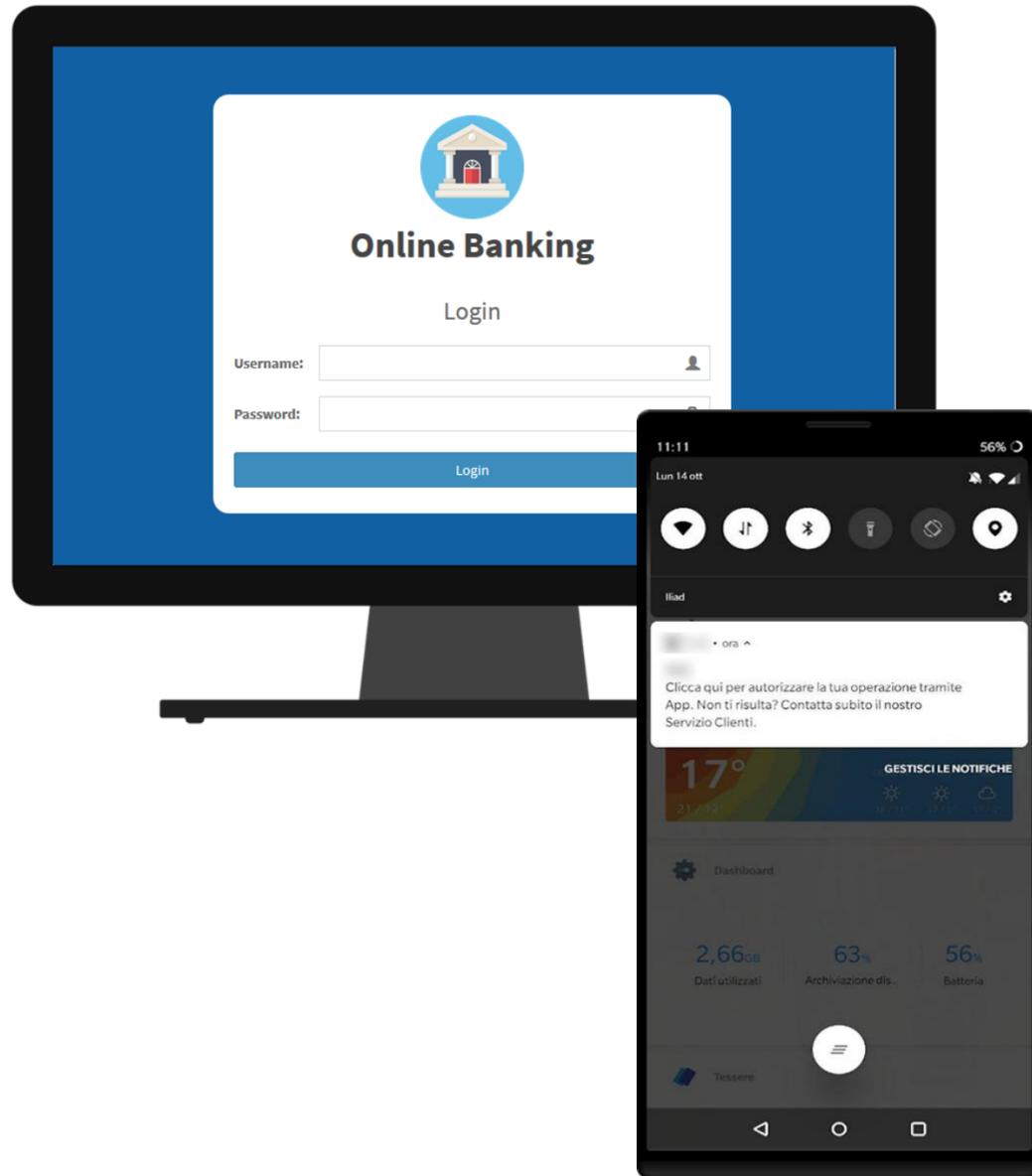
- I insert some secret credentials (e.g., a password on a website)
- I read a value from a list
- I use a device (e.g., a card reader)
- I use a software (e.g., an app on my smartphone)
- I send/receive something on my mobile phone (e.g., an SMS, a Push notification)

Reset Next

Automated Analysis of Security Protocols for the PSD2



MuFASA – Translation



Endpoint: Desktop
Protocol specified so far:



What is your next operation?

- I insert some secret credentials (e.g., a password on a website)
- I read a value from a list
- I use a device (e.g., a card reader)
- I use a software (e.g., an app on my smartphone)
- I send/receive something on my mobile phone (e.g., an SMS, a Push notification)
- None, I'm authenticated

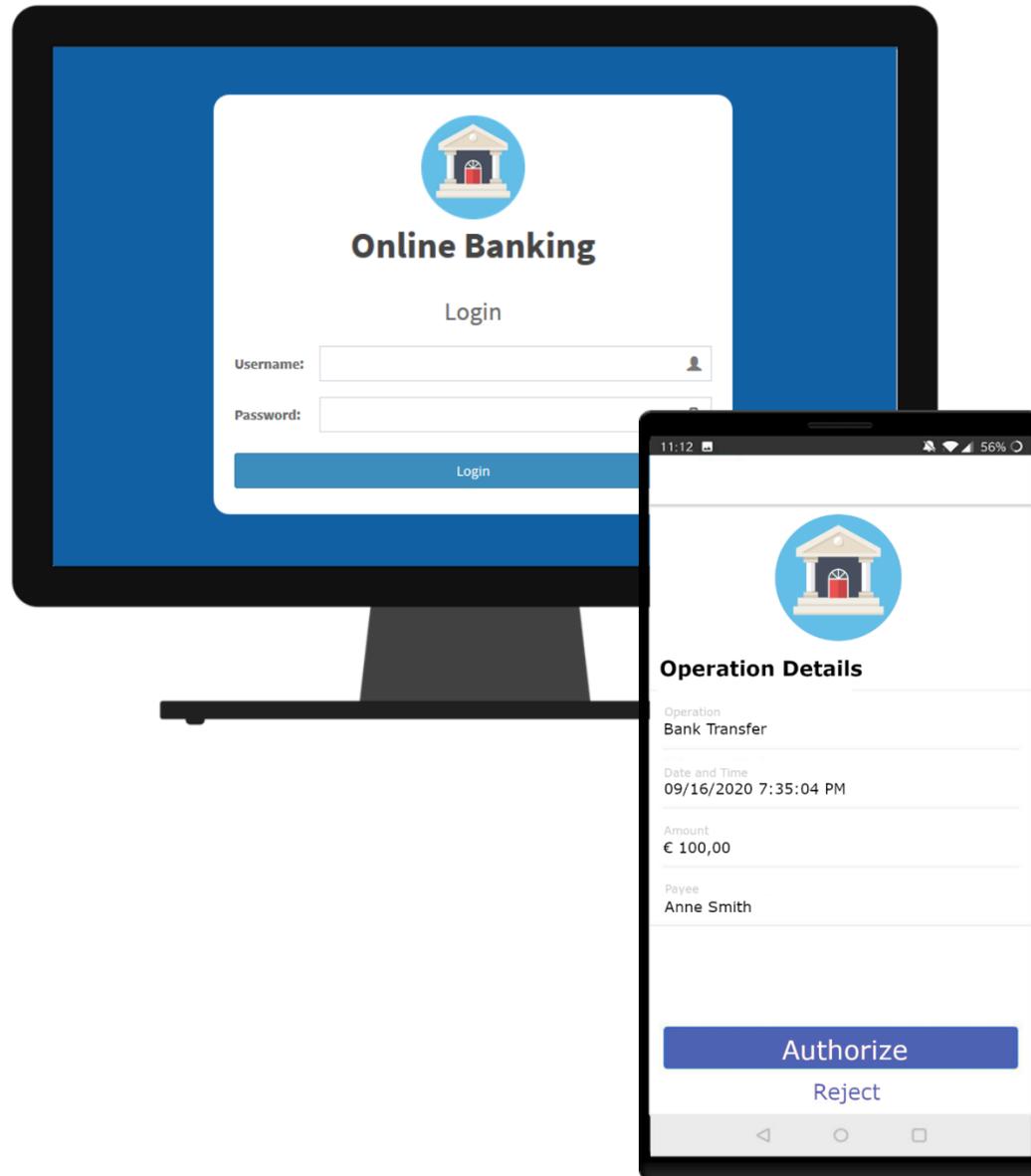
How do you receive information?

- I receive an SMS
- I make a phone call
- I receive a push notification on my smartphone

Automated Analysis of Security Protocols for the PSD2



MuFASA – Translation



Endpoint: Desktop
Protocol specified so far:



What is your next operation?

- I insert some secret credentials (e.g., a password on a website)
- I read a value from a list
- I use a device (e.g., a card reader)
- I use a software (e.g., an app on my smartphone)
- I send/receive something on my mobile phone (e.g., an SMS, a Push notification)
- None, I'm authenticated

How do you receive information?

- I receive an SMS
- I make a phone call
- I receive a push notification on my smartphone

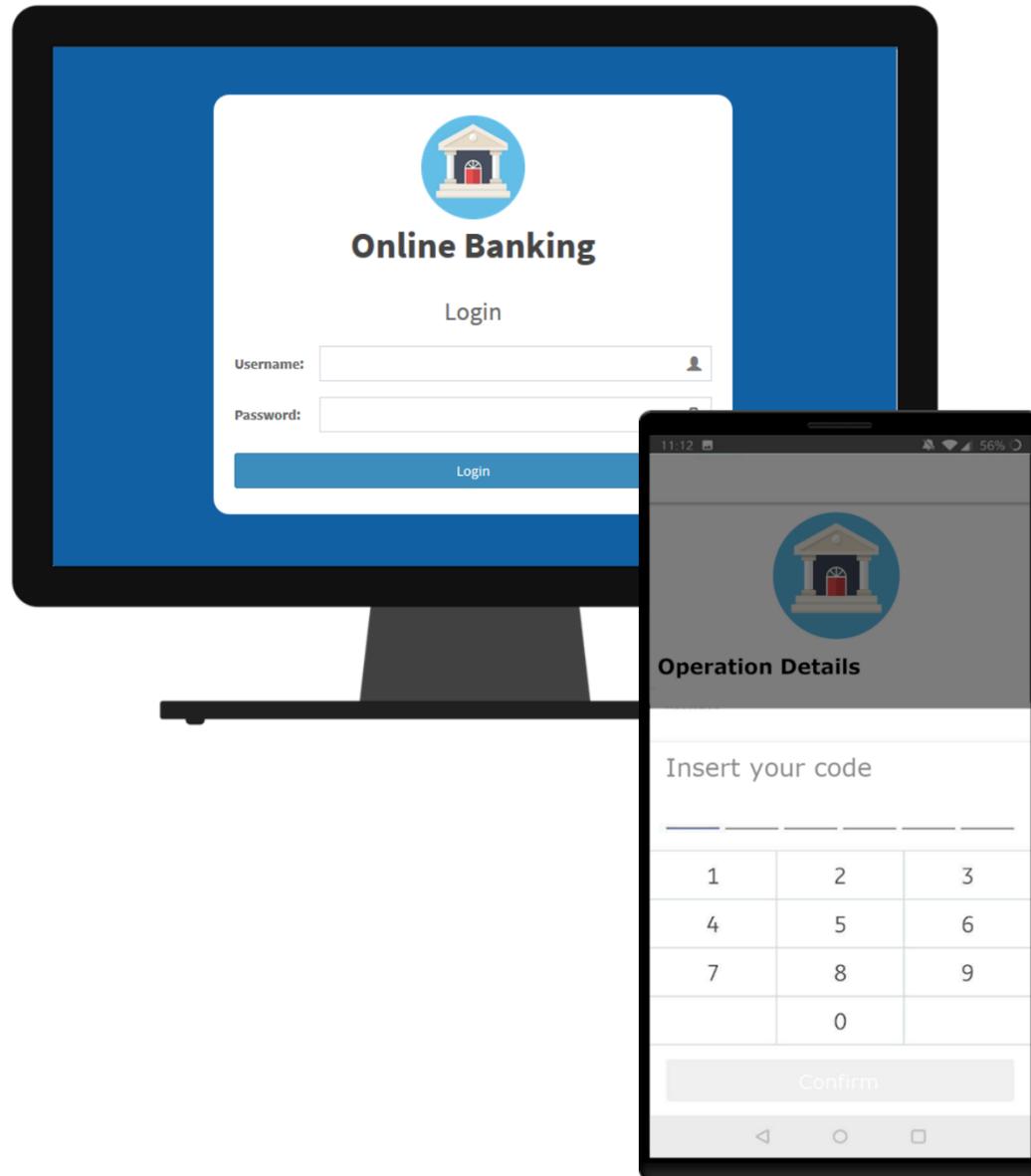
Does it recap the ongoing operation and ask for your confirmation?

- No
- Yes (e.g. You are paying x\$ to y. Confirm?)
- Yes (e.g. You are signing in as ... Confirm?)

Automated Analysis of Security Protocols for the PSD2



MuFASA – Translation



Endpoint: Desktop
Protocol specified so far:



Among the followings, what do you need to use the authenticator?

Nothing

I must insert a secret code/pin

I must scan a part of my body (e.g., my fingerprint)

Does it return some code that you have to copy somewhere?

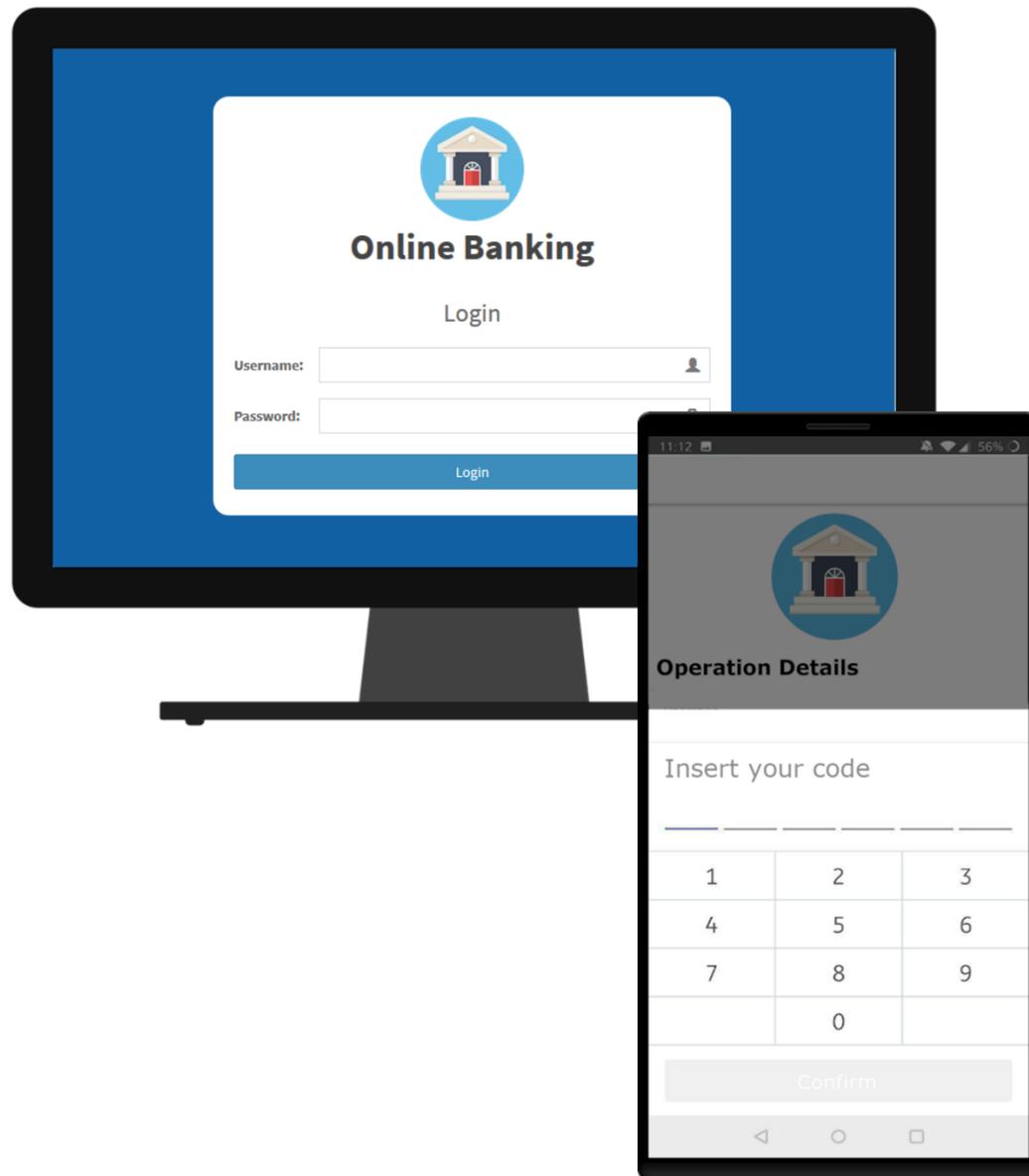
No

Yes

Automated Analysis of Security Protocols for the PSD2



MuFASA – Translation



Endpoint: Desktop
Protocol specified so far:

; opid \gg_n [?] [O,K] \gg_n otp_c

What is your next operation?

- I insert some secret credentials (e.g., a password on a website)
- I read a value from a list
- I use a device (e.g., a card reader)
- I use a software (e.g., an app on my smartphone)
- I send/receive something on my mobile phone (e.g., an SMS, a Push notification)
- None, I'm authenticated

Reset Next

Automated Analysis of Security Protocols for the PSD2

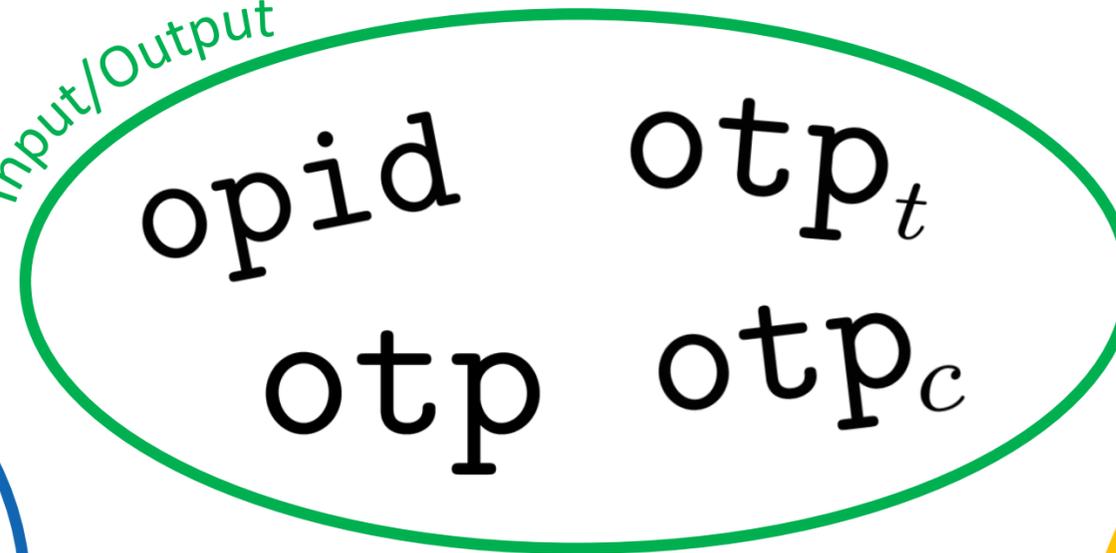


MuFASA – Modeling

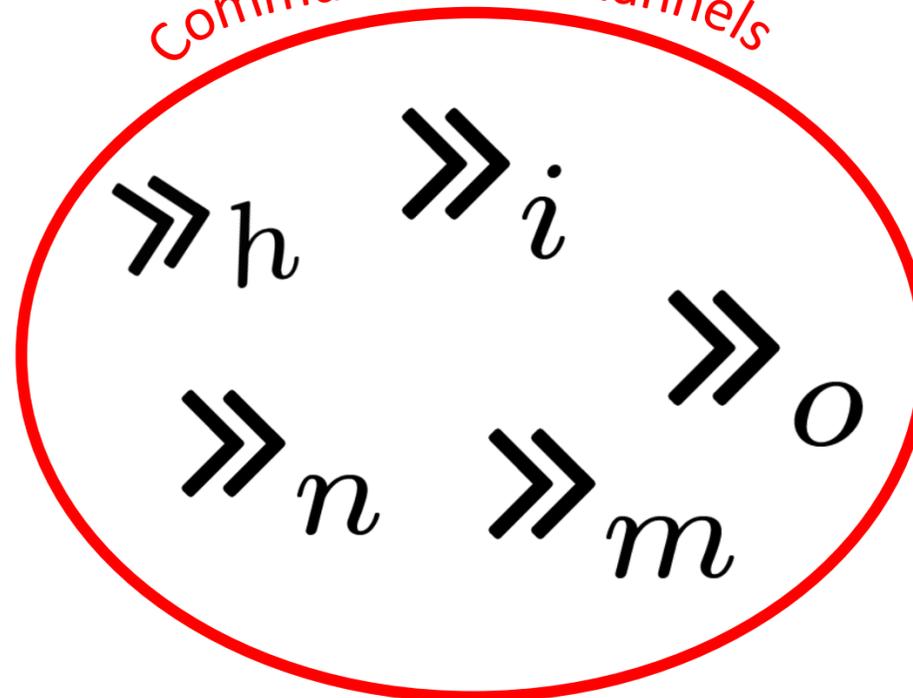
Authenticators



Input/Output



Communication channels



Attackers



Shoulder Surfer: compromises secrets by looking at the victim while typing



Attackers



Man in the Browser: malicious application lying on the victim's browser, manages to tamper with any window or transaction



Social Engineer: deceives the victim into revealing secrets or performing operations



Eavesdropping Software: malicious application intercepting everything is typed on the keyboard



Automated Analysis of Security Protocols for the PSD2



MuFASA – Analysis

Before
PSD2

4 single attackers



After
PSD2

0 single attackers

Automated Analysis of Security Protocols for the PSD2



MuFASA – Analysis

Before
PSD2

4 single attackers

After
PSD2

0 single attackers

Advantages:

Security:

- the user is aware of the ongoing operation
- the authentication code is connected with the ongoing operation and session, therefore it cannot be used anywhere nor for any other operation
- the authentication code is sent directly through the network, without requiring the user to manually enter it → attackers that intercept the code while the user is typing are mitigated

Dynamic Linking

Usability: common devices are leveraged (smartphone)

Automated Analysis of Security Protocols for the PSD2



MuFASA – Reporting

Analysis of MFA Protocol

$Q; \text{opid} \gg_n \text{[O,K]} \gg_n \text{otp}_c$

Info on the Analyzed Protocol:

- Starting Endpoint: Desktop
- Number of authenticators: 2
- Employed authentication factors: [K, K, O]

Protocol Complexity

- Memory: 2
- Manual Operations: 0
- Extra Devices: 0
- **Complexity Score: 2**

Compliance with security requirements

- Requirement 1: true
- Requirement 2: true
- Requirement 3: true
- Requirement 4: true

Result of the resistance analysis

Base attackers: DT, AD, SS, ES, SE, MB, MM
 Max number of attackers in combination: 3
 Considered attackers: 63

Combinations of attackers
DT SS
ES MM
MM MB
ES DT
SS AD
ES AD
SS MM
MM SE

Automated Analysis of Security Protocols for the PSD2

Security Analysis

To detect the attackers that manage to compromise the protocol, we perform two different kinds of analysis:

1. **Combinatorial Analysis:** relying on attackers' capabilities on the authentication factors. It is fast and thus helps prune the set of attackers to test, but may not detect some advanced attacks.
2. **Formal Analysis:** relying on formal methods (a specification language and a model checker). It can be computationally expensive, but manages to find even more complex categories of attacks.

Automated Analysis of Security Protocols for the PSD2

Formal Analysis with ASlan++ and SATMC

```
entity IdPServer(Actor, FCMServer, EICApp, User, SPSServer, Browser, EIC: agent, Ch_B2IdPS, Ch_IdPS2FCMSrv, Ch_EICApp2IdPS, Ch_IdPS2EICApp: channel) {
```

```
symbols
```

```
IdPCookie: cookie;
OpId: opid;
Request: userrequest;
```

```
body { % of IdPServer
```

```
select {
```

```
on(Browser -Ch_B2IdPS-> Actor: ?Request):{
  Actor -Ch_IdPS2B-> Browser: Actor;
```

```
select {
```

```
on(Browser -Ch_B2IdPS-> Actor: User.?IdPCookie &
  enrollmentDB(Actor)->contains((User,?IdPCookie))):{
  OpId := fresh();
  Actor -Ch_IdPS2FCMSrv-> FCMServer: OpId.Request;
```

```
select {
```

```
on(EICApp -Ch_EICApp2IdPS-> Actor: OpId):{
  Actor -Ch_IdPS2EICApp-> EICApp: OpId.Actor.SPSServer;
```

```
select {
```

```
on(EICApp -Ch_EICApp2IdPS-> Actor: OpId.{OpId.Actor.SPSServer}_inv(pk(EIC))):{
  Actor -Ch_IdPS2B-> Browser: {Actor.User.SPSServer}_inv(pk(Actor));
```

```
}
```

```
}
```

```
}
```

```
}
```

```
}
```

```
}
```

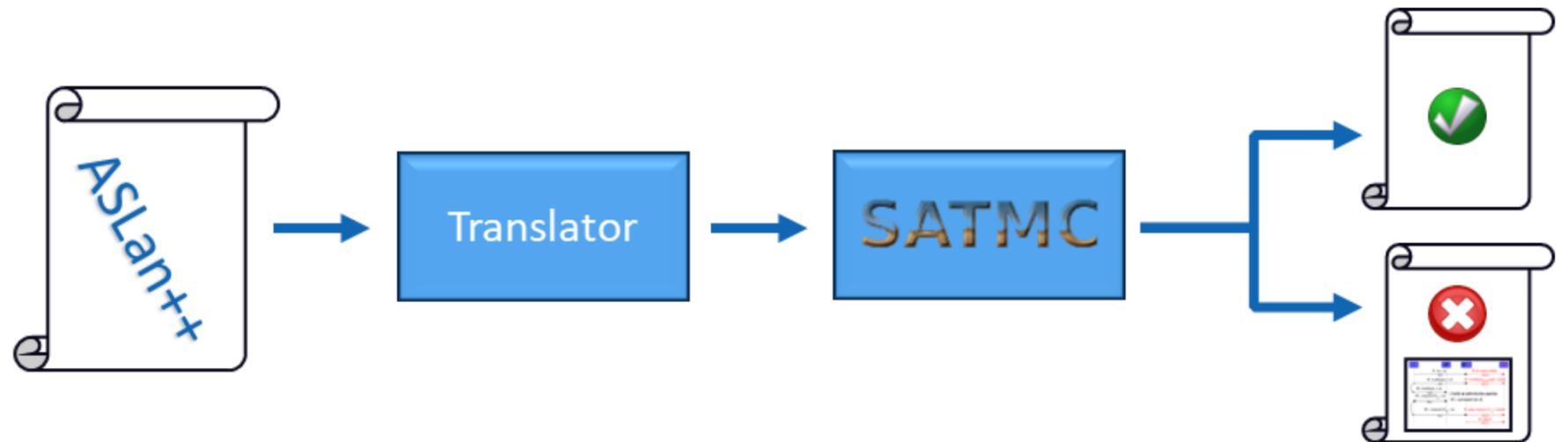
```
}
```

```
}
```

```
}
```

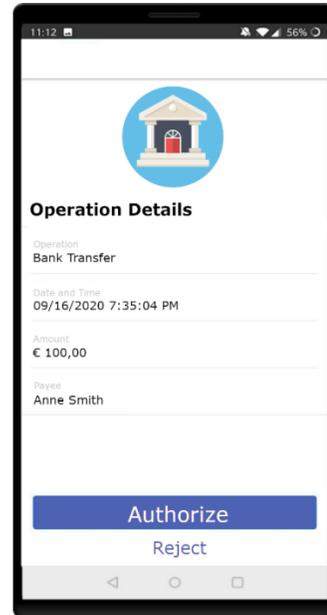
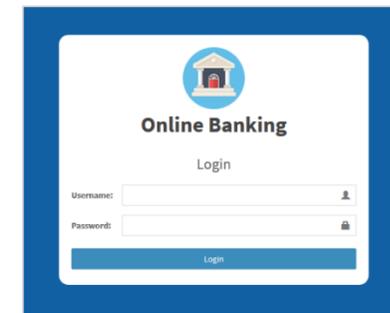
```
}
```

```
}
```



Advanced Vulnerabilities

Man in the Browser (Login)



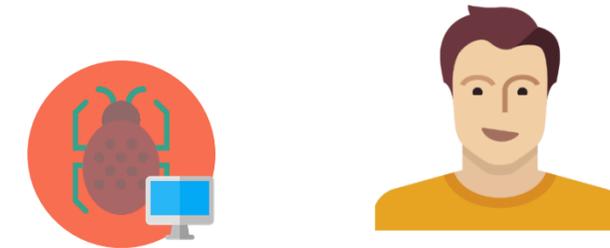
Advanced Vulnerabilities

Man in the Browser (Login)



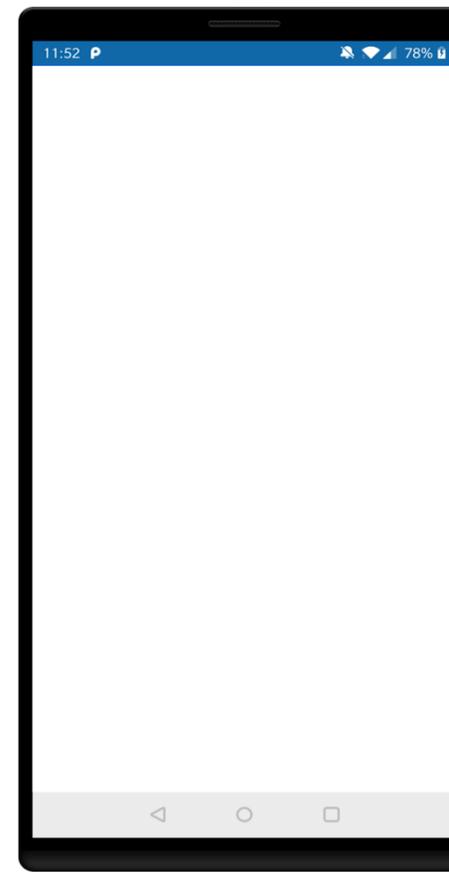
Advanced Vulnerabilities

Man in the Browser (Login)



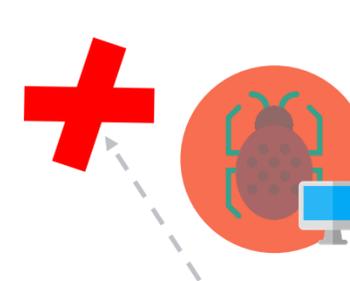
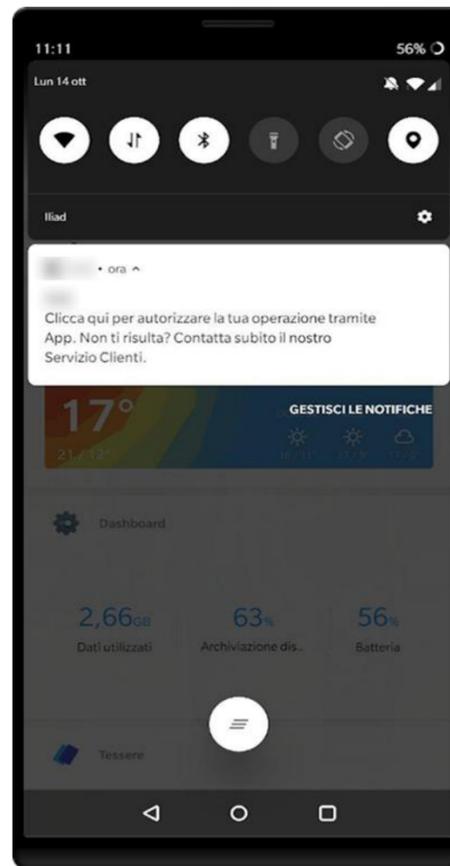
Advanced Vulnerabilities

Man in the Browser (Login)



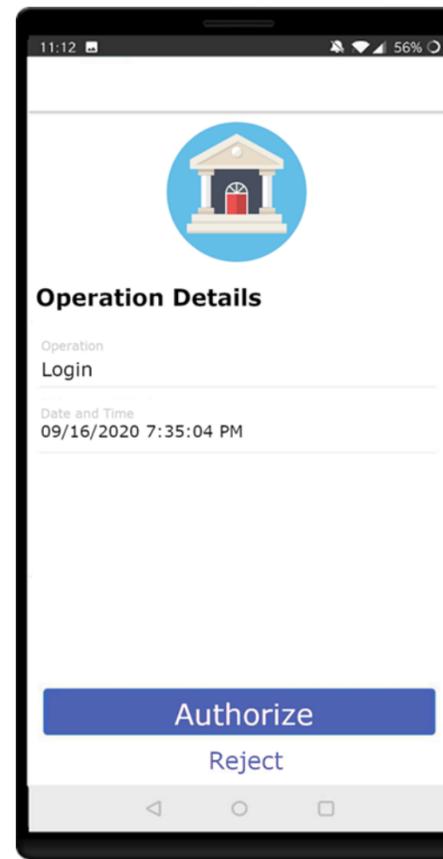
Advanced Vulnerabilities

Man in the Browser (Login)



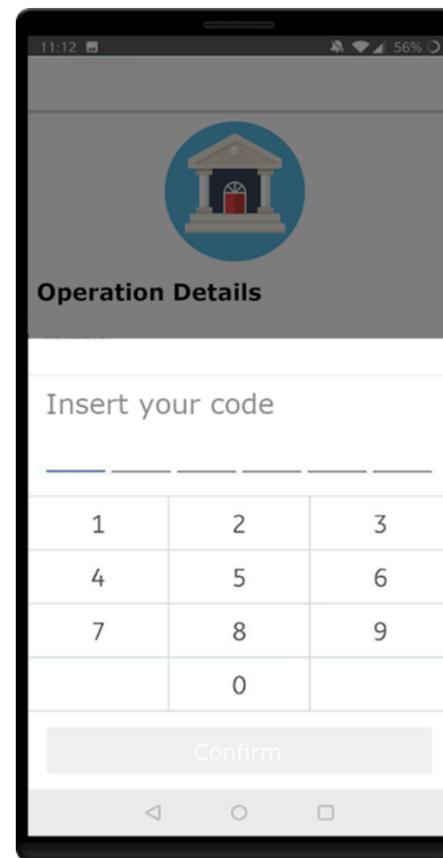
Advanced Vulnerabilities

Man in the Browser (Login)



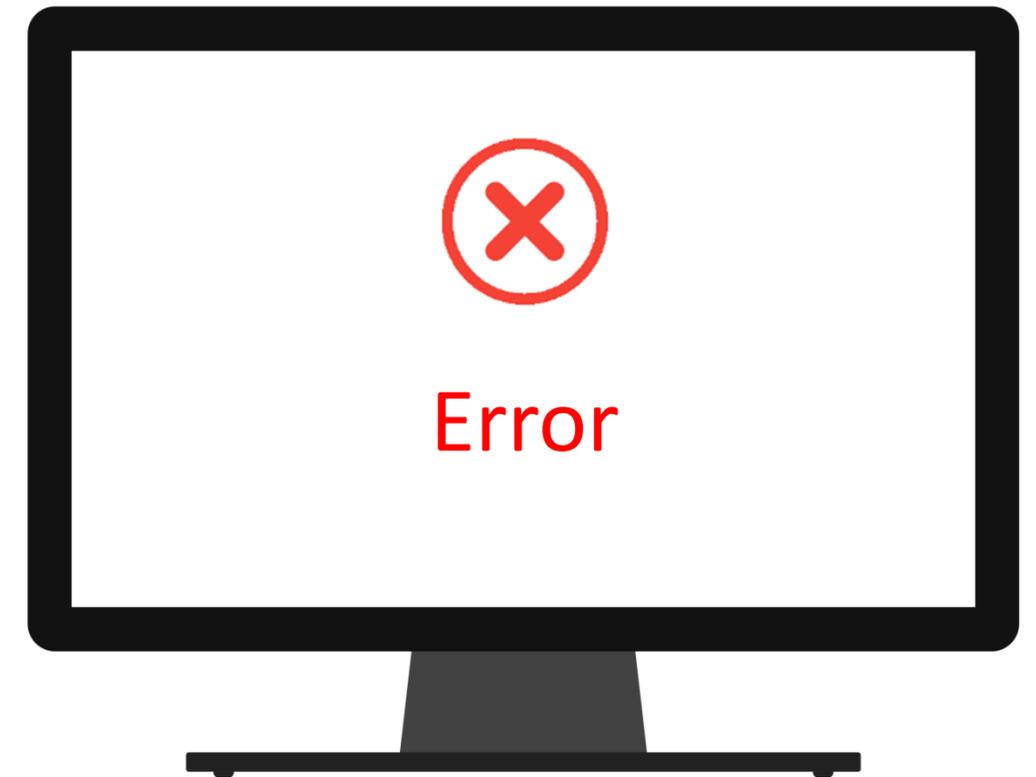
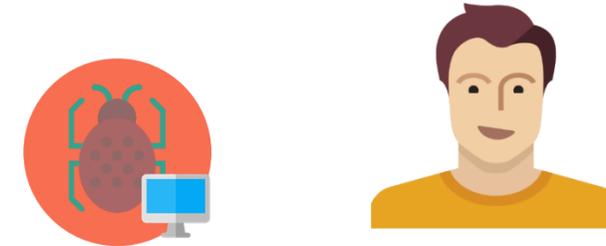
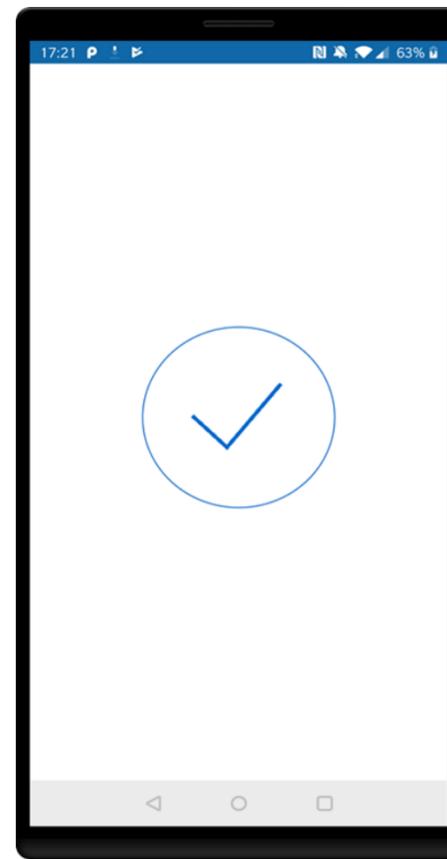
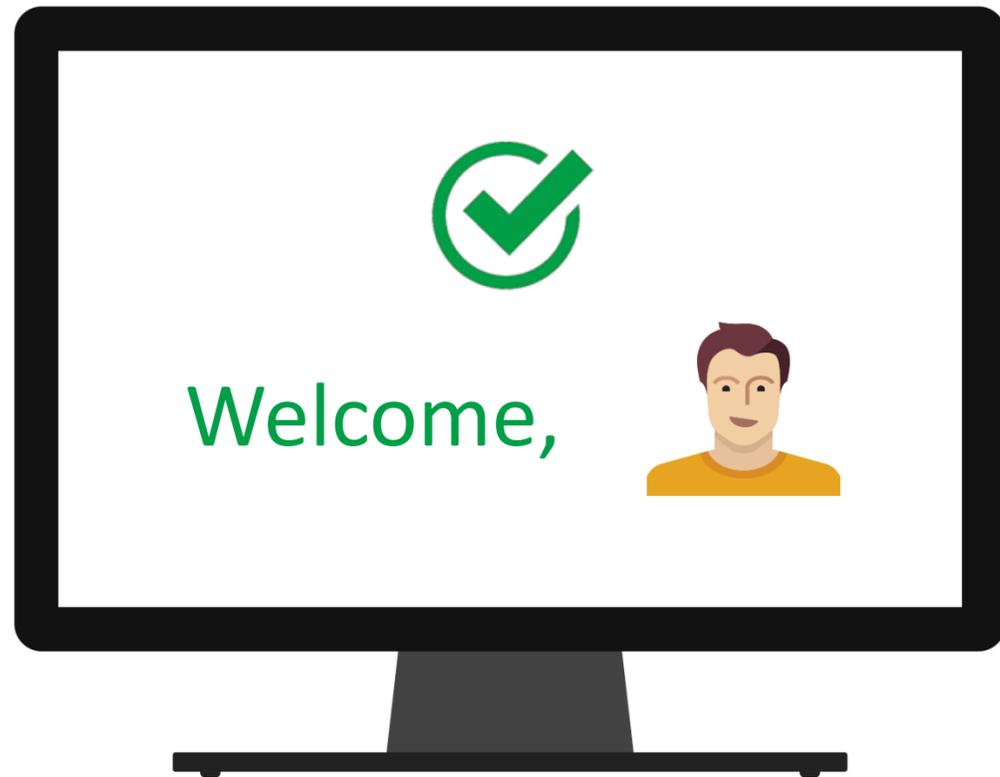
Advanced Vulnerabilities

Man in the Browser (Login)

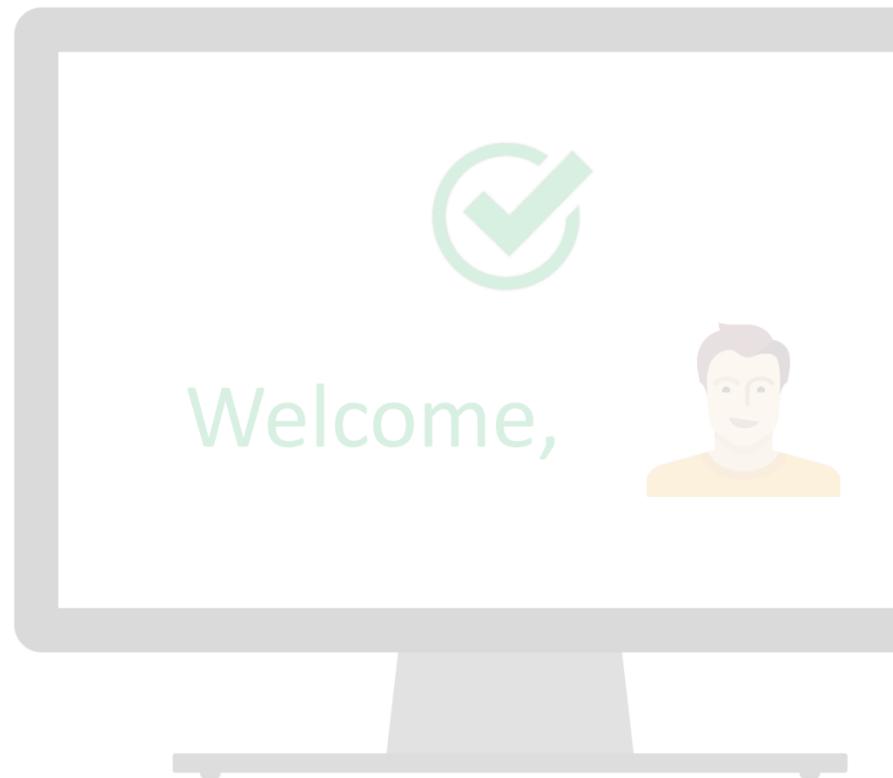


Advanced Vulnerabilities

Man in the Browser (Login)



Advanced Vulnerability Man in the Browser



Operation Details

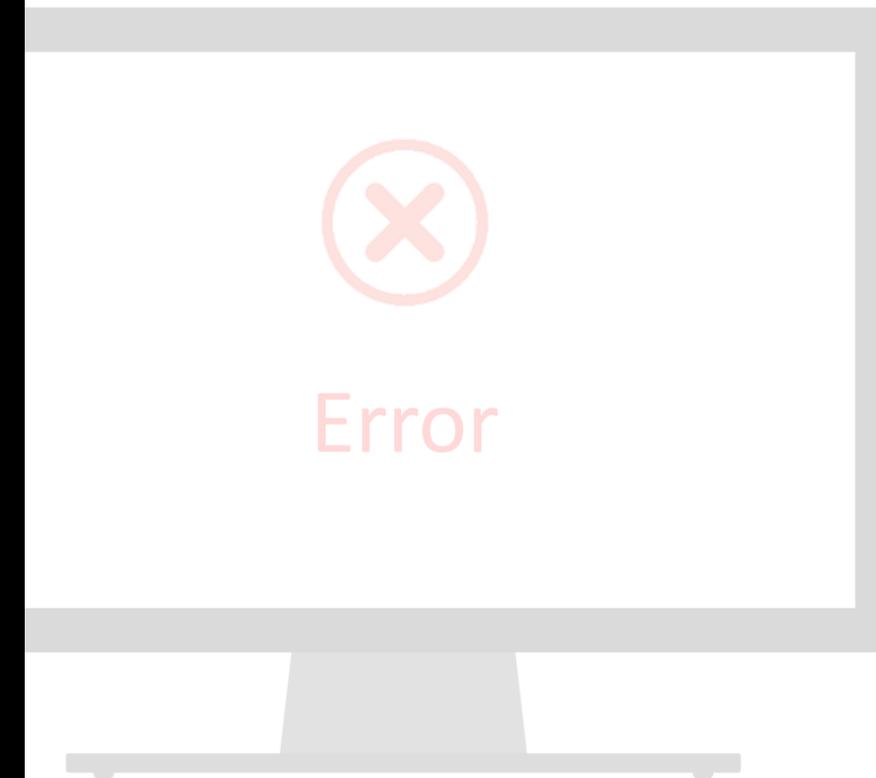
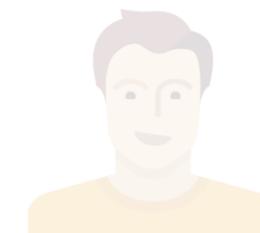
Operation

Login

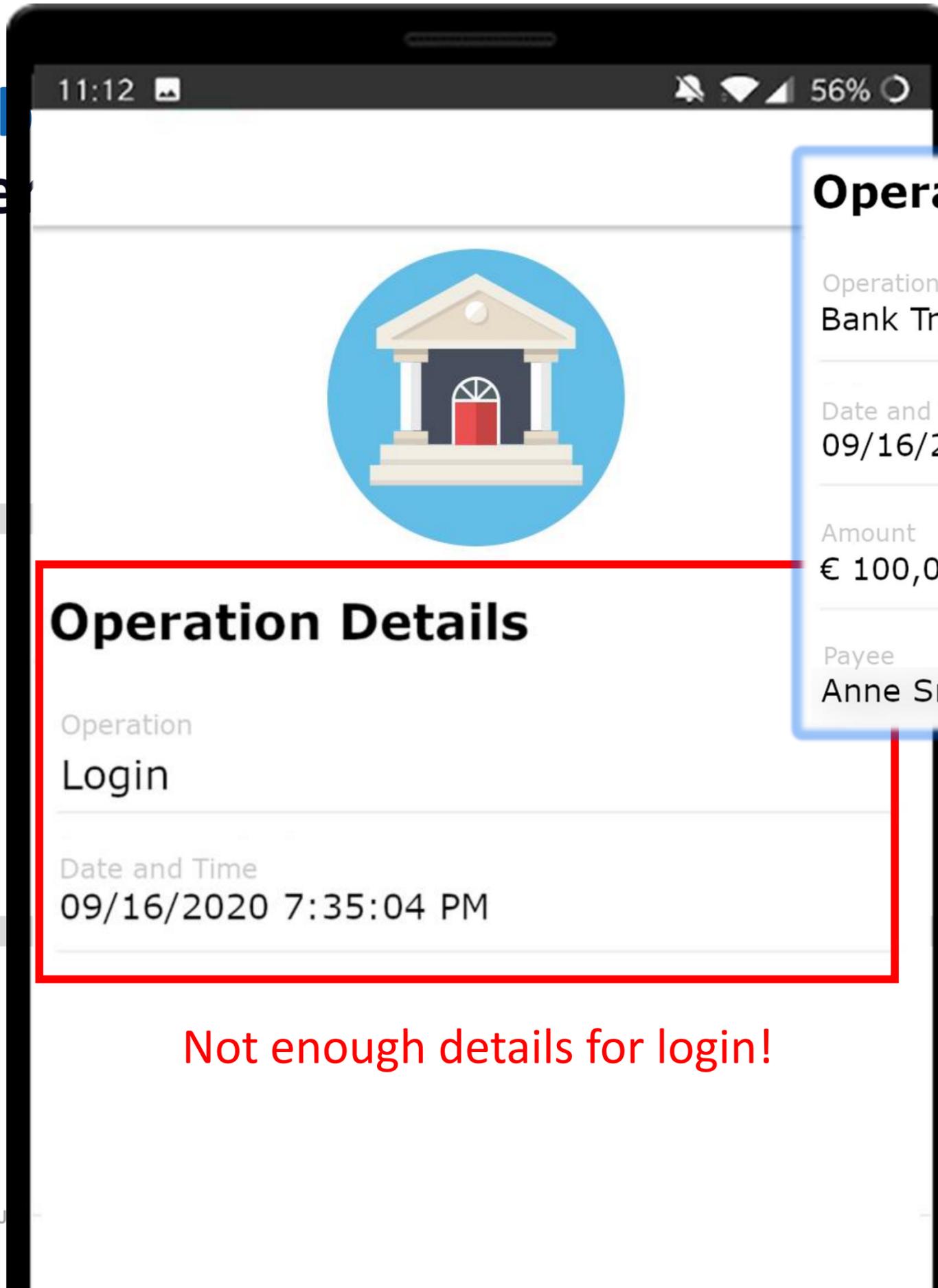
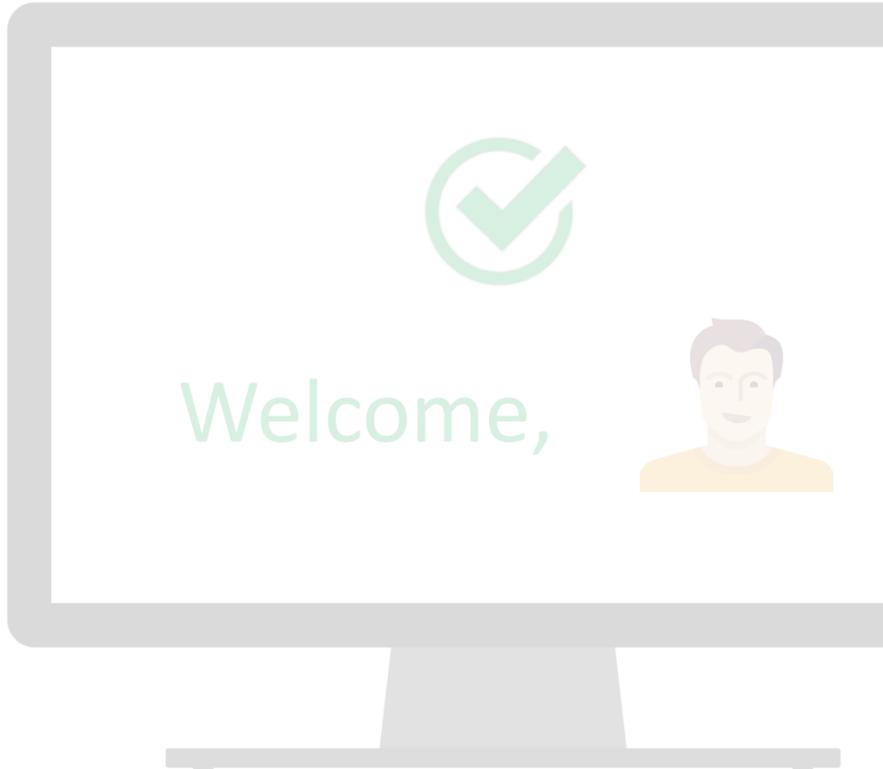
Date and Time

09/16/2020 7:35:04 PM

Not enough details for login!



Advanced Vulnerability Man in the Browser



Operation Details

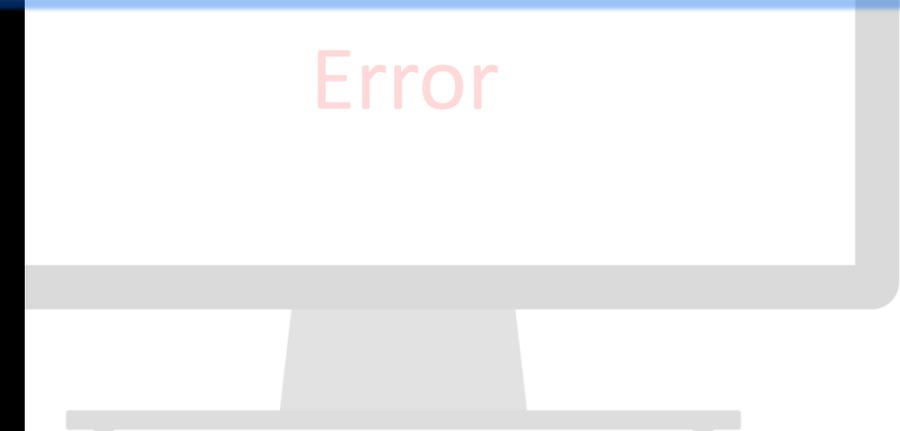
Operation
Bank Transfer

Date and Time
09/16/2020 7:35:04 PM

Amount
€ 100,00

Payee
Anne Smith

Enough information for operation authorization!



Not enough details for login!

Automated Analysis of Security Protocols for the PSD2

A Two-Levels Approach

1

Security Analysis

To detect the attackers that manage to compromise the protocol

2

Risk Analysis

To evaluate the risks connected with the successful attackers detected

Automated Analysis of Security Protocols for the PSD2

Risk Analysis with OWASP Risk Rating Methodology



Likelihood

Impact

$$\text{Risk} = \text{Likelihood} \times \text{Impact}$$

Probability of an attack happening

Consequences in case of the attack was successful

Automated Analysis of Security Protocols for the PSD2

Risk Analysis with OWASP Risk Rating Methodology

		Likelihood		
		<i>Low</i>	<i>Medium</i>	<i>High</i>
Impact	<i>Low</i>	Note	Low	Medium
	<i>Medium</i>	Low	Medium	High
	<i>High</i>	Medium	High	Critical

$$\text{Risk} = \text{Likelihood} \times \text{Impact}$$

Probability of an attack happening

Consequences in case of the attack was successful

Automated Analysis of Security Protocols for the PSD2

Risk Analysis with OWASP Risk Rating Methodology

Result of the resistance analysis

Base attackers: DT, AD, SS, ES, SE, MB, MM

Max number of attackers in combination: 3

Considered attackers: 63

Combinations of attackers	Likelihood	Impact	Risk
DT SS	MEDIUM	MEDIUM	MEDIUM
ES MM	LOW	HIGH	MEDIUM
MM MB	LOW	HIGH	MEDIUM
ES DT	LOW	MEDIUM	LOW
SS AD	LOW	MEDIUM	LOW
ES AD	LOW	MEDIUM	LOW
SS MM	LOW	MEDIUM	LOW
MM SE	LOW	MEDIUM	LOW



Questions?

Thank you for the attention!



Marco Pernpruner
mpernpruner@fbk.eu

 <https://stfbk.github.io>