

*The Trusted Source for  
Secure Identity Solutions*

# Le monde bancaire à l'heure de la révolution Open Banking et DSP2

Quel impact sur la sécurité ?

Olivier Thirion de Briel – HID Global

# What is PSD?

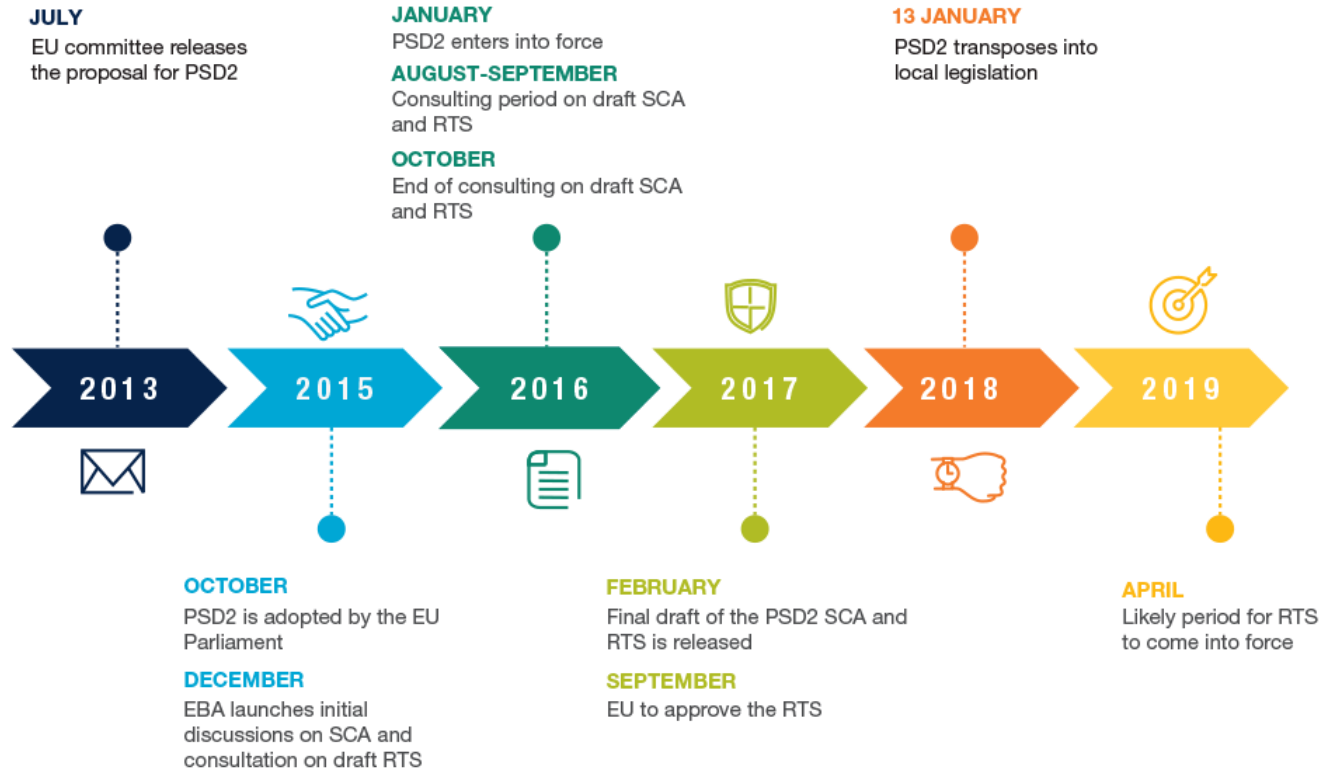
- PSD1: Payment Services Directive
  - The 'market rules' describe which type of organizations can provide payment services.
  - The 'business conduct rules' specify
    - what transparency of information payment service institutions need to provide, including any charges, exchange rates, transaction references and maximum execution time.
    - the rights and obligations for both payment service providers and users,
    - how to authorize and execute transactions,
    - liability in case of unauthorized use of payment instruments,
    - refunds on payments,
    - revoking payment orders,
    - value dating of payments.

# Why PSD2?

- Important growth of online fraud
- Need for more competition
- Better protect the consumer
- Inconsistency in the application of PSD1
- Many unregulated players
- Lack of standardisation

The new directive focuses mainly on  
**security, transparency, and innovation**

# EU - PSD2



Source: Capgemini Financial Services Analysis, 2017; SME Inputs

Banks have a little more than a year to comply with the PSD2 requirements.  
=> PSD2 is becoming a real focus for Banks

# PSD2 scope

## Introduction of new stakeholders: TPP (Third Party Providers)

- **AISP**: Account Information Service Provider will be able to access bank account information, including history and balances, of users which gave consensus
- **PISP**: Payment Initiation Service Providers will allow users to initiate online payments to a beneficiary as an alternative to the use of payment cards in online transactions

## Security and authentication

- PSD2 introduces **new security requirements** for electronic payments and account access along with new security challenges relating to AISPs and PISPs

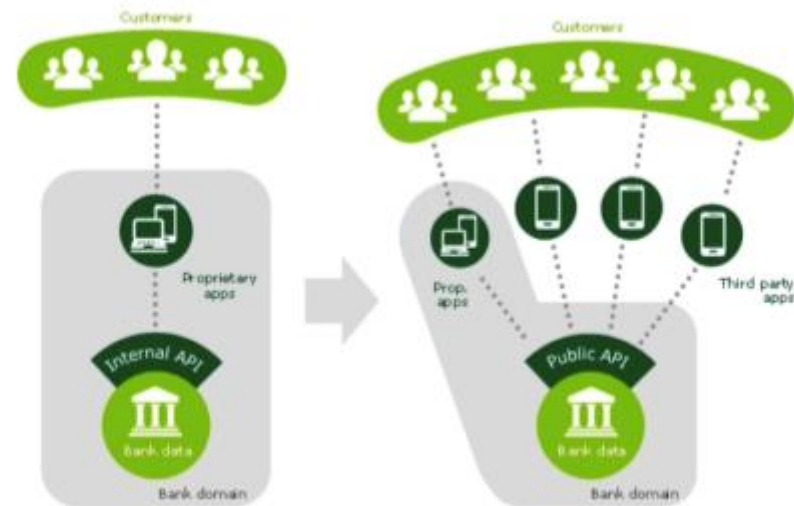
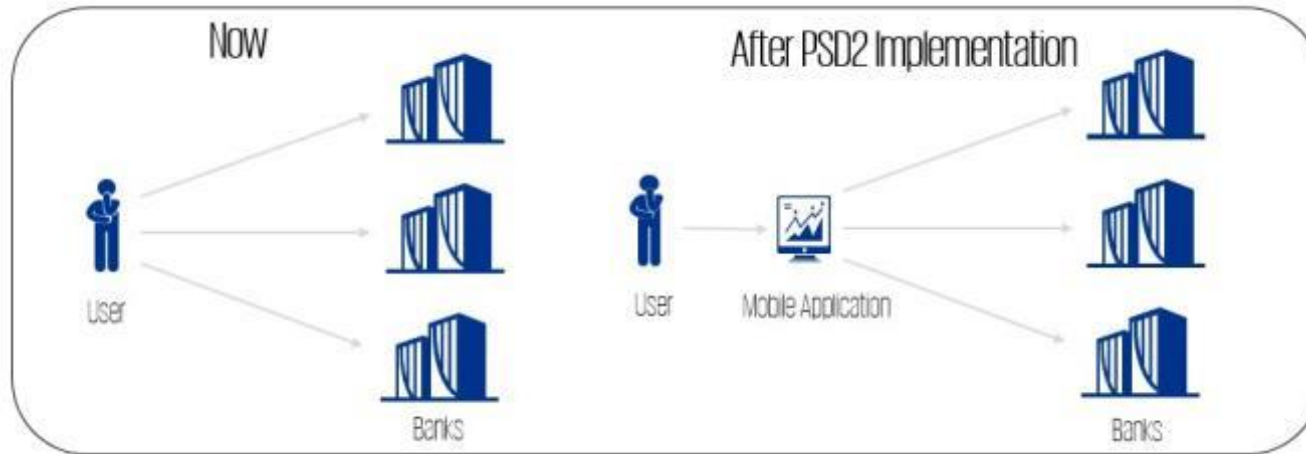
## Extension

- Extension of scope beyond Europe by **including "one leg out" transactions** and in the definition of a "Payment Institution"

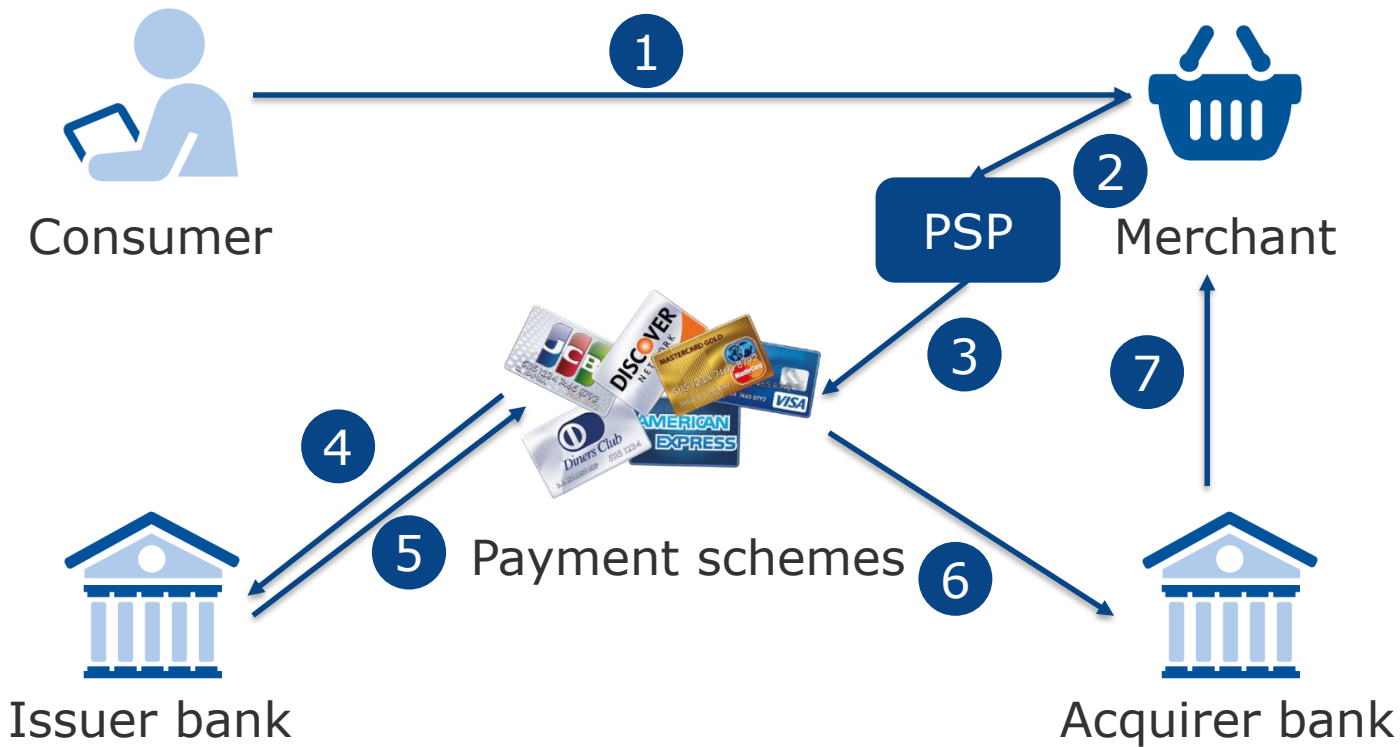
## Prohibition of card surcharges

- PSD2 seeks to standardize the different approaches to surcharges on card-based transactions

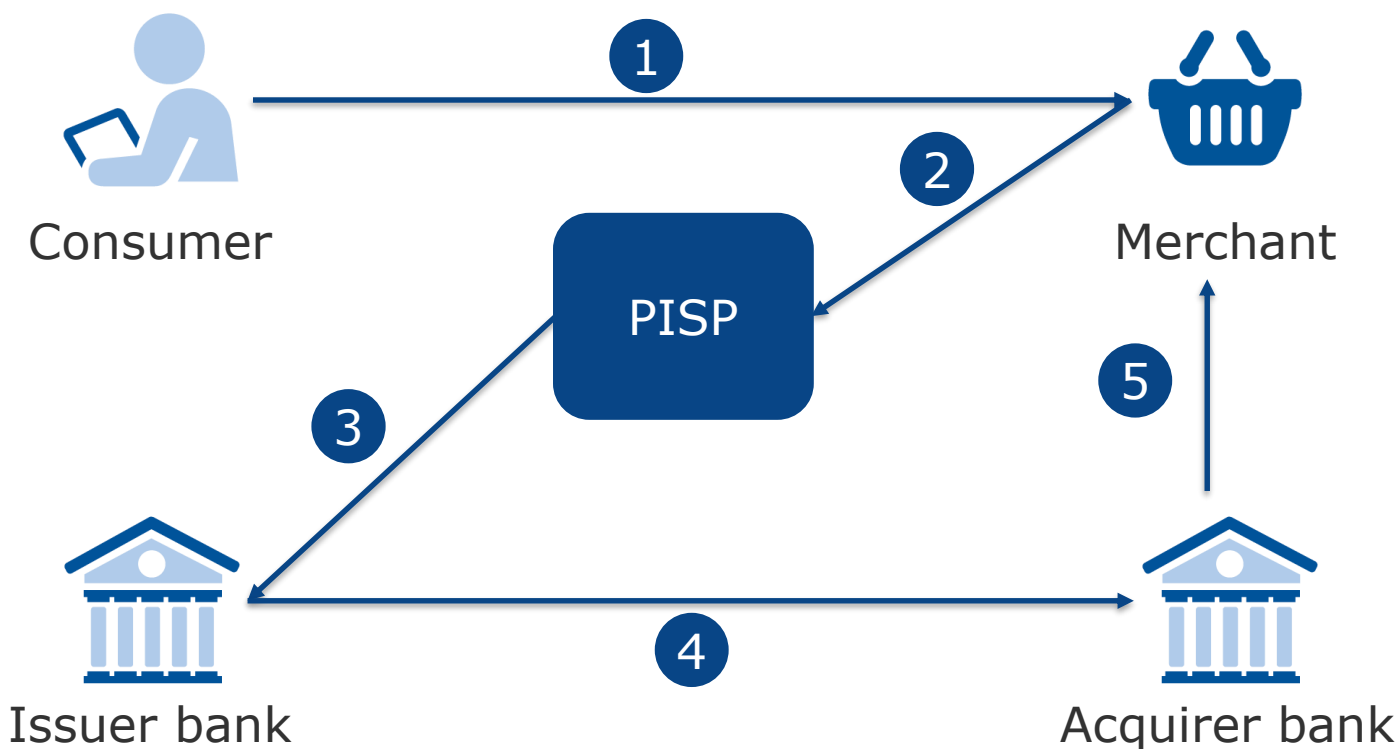
# AISP (Account Information Service Provider)



# PISP (Payment Initiation Service Provider), before PSD2



# PISP (Payment Initiation Service Provider), with PSD2





# Strong authentication in PSD2

- payment service provider, AISP and PISP apply strong customer authentication (SCA) where the payer:
  - a) accesses its payment account online;
  - b) initiates an electronic payment transaction;
  - c) carries out any action through a remote channel which may imply a risk of payment fraud or other abuses.
- With regard to the initiation of electronic payment transactions, payment service providers and PISP apply strong customer authentication that includes elements which dynamically link the transaction to a specific amount and a specific payee.

Knowledge



possession



inherence



# HID Global device portfolio PSD2 compliance checking

| Device   | Functions   | Dynamic linking   | Sanity check  | Cloning protection  | Independence  | PSD2 compliance  |
|--|---|---|---|---|---|--|
|   | 1 button HW token/smartcard<br><i>Possession</i> : HW token<br><i>Knowledge</i> : Password  |    | N/A   |    |    | <b>YES</b> , for authentication procedure and authentication code only |
|    | Keypad HW token<br><i>Possession</i> : HW token<br><i>Knowledge</i> : PIN/Password  |    | N/A   |    |    | <b>YES</b> , for all use cases   |
|  Transaction on different device           | Mobile authentication application with mobile application security<br><i>Possession</i> : Mobile<br><i>Knowledge</i> : PIN/Password<br><i>Inherence</i> : Fingerprint |    |    |    |    | <b>YES</b> , for all use cases   |
|  Transaction on same device, different app | Mobile authentication application with mobile application security<br><i>Possession</i> : Mobile<br><i>Knowledge</i> : PIN/Password<br><i>Inherence</i> : Fingerprint |    |    |    |    | <b>YES</b> , for all use cases   |
|  Transaction on different device          | Mobile SDK with mobile application security<br><i>Possession</i> : Mobile<br><i>Knowledge</i> : PIN/Password<br><i>Inherence</i> : Fingerprint                        |   |   |   |   | <b>YES</b> , for all use cases   |
|  Transaction on same device, same app    | Mobile SDK with mobile application security<br><i>Possession</i> : Mobile<br><i>Knowledge</i> : PIN/Password<br><i>Inherence</i> : Fingerprint                        |  |  |  |  | <b>YES</b> , for all use cases   |

# APIs

- Banks have to provide to AISP and PISP access to their online account/payment service
  - This includes an 'Access to Accounts' (XS2A) rule, which will force Banks/ PSPs to **facilitate secure access through API to their customer accounts and provide account information to third party apps**, if the account holder wishes to do so



Banks risk to lose contact with their end-users,  
due to those new intermediaries

# Which APIs?

## (AISP) Account Information Service Provider

Authentication & Authorisation

Account Balance

Transaction History

## (PISP) Payment Initiation Service Provider

Authentication & Authorisation

Sufficient Funds

Account Balance

Payment Initiation

# Open API

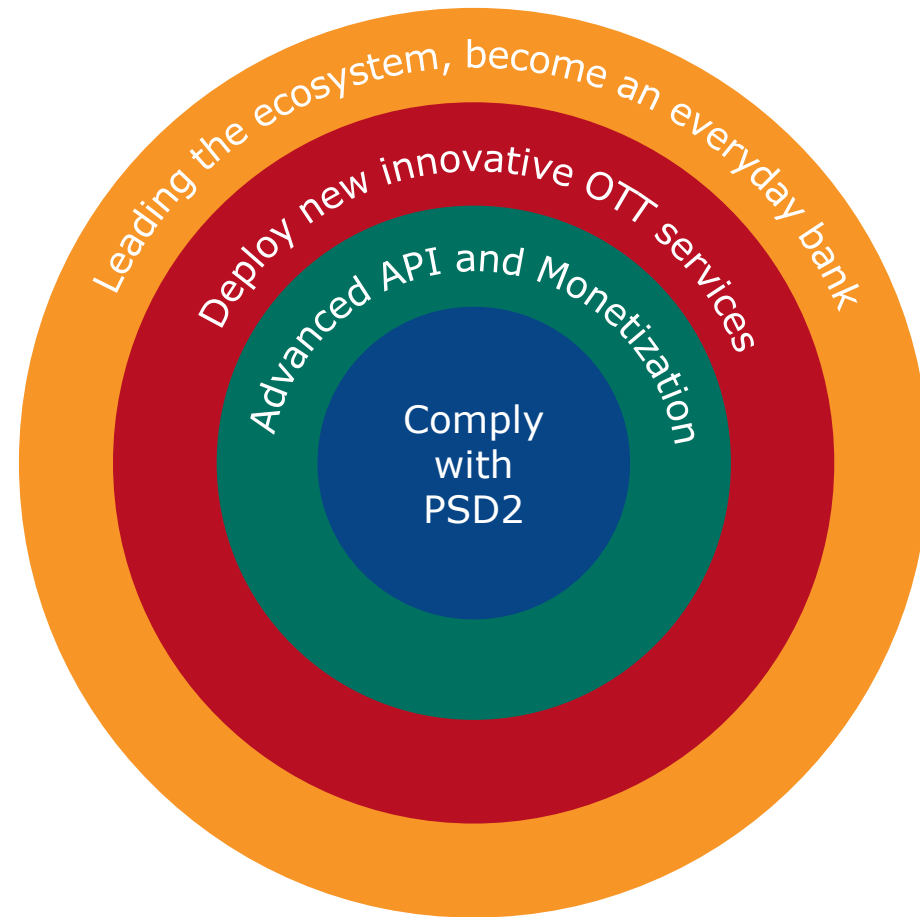
## Opportunities

- New product and services
- Better customer experience
- Regulation compliancy
- Better customer insights

## Threats

- Commoditization of banking processes
- Disintermediation
- Losing business
- Open door to hackers

# PSD2, a real challenge for banks



# Banks' assets



Trust



Data



Interconnexion



Infrastructure



Compliance

Banks have all the assets  
to build digital trusted identities

# Banking evolution

**Central identity  
and  
authentication  
provider**

**for the  
connected  
world**







A global leader in trusted identity solutions

25+ years of market leadership

Based in Austin, Texas

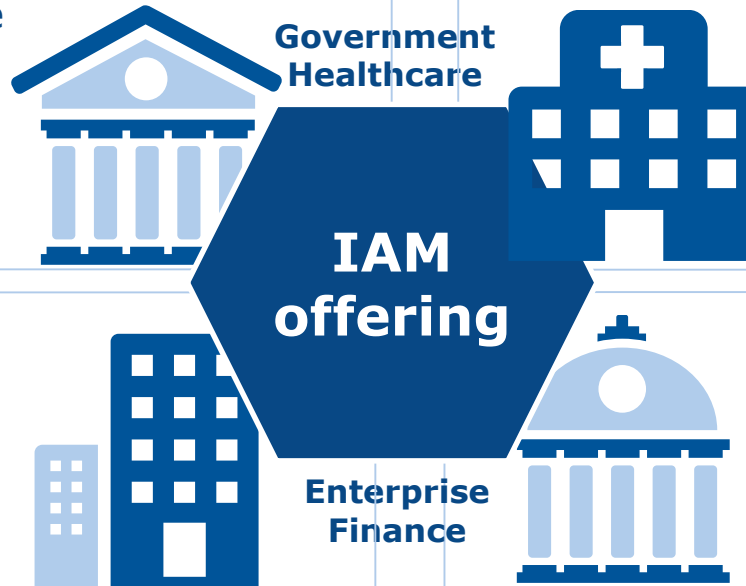
3,000 employees worldwide

HID Global is an ASSA ABLOY Brand

# The broadest portfolio to best meet your needs

## Physical Identity and Access Management

Convergence of PACS systems & digital space



## Identity Lifecycle Credential Management System



Trust Network for  
3rd party transactions  
**Certification  
Authority**



Digital Access &  
remote transactions  
**Authentication**

# HID IAM: We Power Trusted Identities

**Millions**  
Identities Managed



**6 billion+**  
Payment transactions  
protected last year



**2 billion+**  
Things connected with  
HID technologies



**4.8 million+**  
Device identities protected



**800 million+**  
Certificate validations in  
the last year



# About ASSA ABLOY



ASSA ABLOY is  
***the global leader in  
door opening solutions.***

An 8 billion Euro  
company based  
in Stockholm

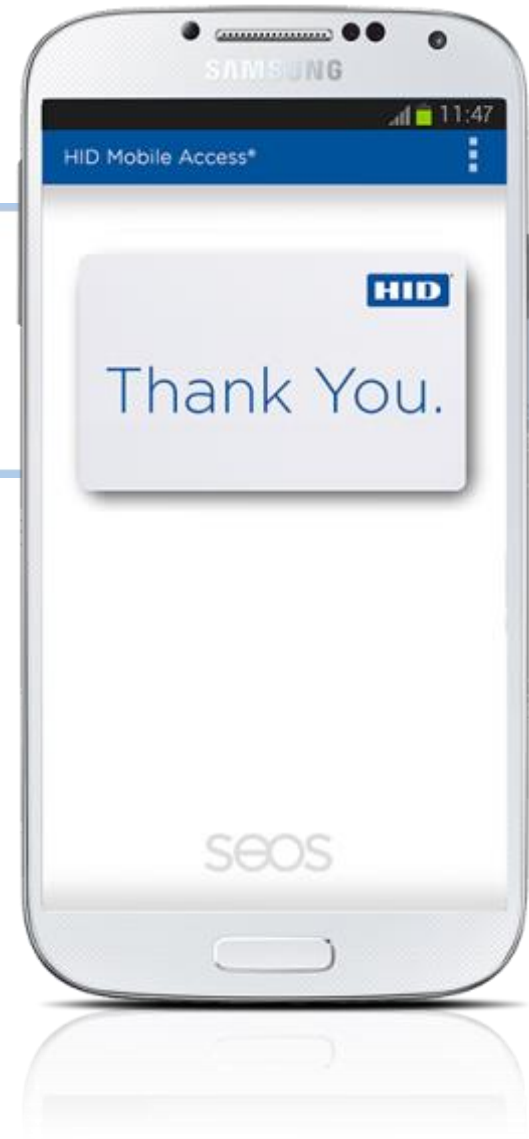


46,000  
employees  
worldwide



hidglobal.com

Olivier Thirion de Briel  
Othiriondebriel@hidglobal.com



PROPRIETARY INFORMATION. Do not reproduce, distribute, or disclose. No unauthorized use.







# Exemptions

- SCA is not mandatory in the following cases:
  - For payment account information consultation, except:
    - For the first time
    - Every 90 days
  - For contactless payments at POS, when:
    - The amount of the payment does not exceed 50€
    - The cumulative amount on the last transactions doesn't exceed 150€ or the user hasn't done 5 consecutive contactless payments
  - For remote electronic payment, when:
    - The amount of the payment does not exceed 30€
    - The cumulative amount on the last transactions doesn't exceed 100€ or the user hasn't done 5 consecutive contactless payments
    - The level of risk is low depending on the fraud rate of the PISP and on the amount of the transaction, up to 500€
- Full exemption:
  - Unattended payment terminals (for transport and parking fares)
  - Trusted beneficiaries and recurring transactions (except for creation)
  - Payments to yourself if both accounts are in the same bank

# Some definitions

- **Strong Customer Authentication (SCA):** standard 2FA
- **Dynamic linking:**
  1. *"the payer is made aware of the amount of the payment transaction and of the payee;*
  2. *the authentication code generated shall be specific to the amount of the payment transaction and the payee agreed to by the payer when initiating the transaction.*
  3. *the authentication code accepted by the payment service provider corresponds to the original specific amount of the payment transaction and to the payee agreed to by the payer. Any change to the amount or the payee shall result in the invalidation of the authentication code generated."*
- **Cloning protection:** *"The use by the payer of elements categorized as possession shall be subject to measures designed to prevent replication of the elements"*
- **Independence & Sanity check:**
  1. *"Payment service providers shall ensure that the use of the elements of strong customer authentication shall be subject to measures in terms of technology, algorithms and parameters, which ensure that the breach of one of the elements does not compromise the reliability of the other elements.*
  2. *Where any of the elements of strong customer authentication or the authentication code is used through a multi-purpose device including mobile phones and tablets, payment service providers shall adopt security measures to mitigate the risk resulting from the multi-purpose device being compromised.*
  3. *For the purposes of paragraph 2, the mitigating measures shall include each of the following:*
    - *the use of separated secure execution environments through the software installed inside the multi-purpose device;*
    - *mechanisms to ensure that the software or device has not been altered by the payer or by a third party or mechanisms to mitigate the consequences of such alteration where this has taken place."*

# Stakeholders reactions

| Stakeholder  | Reaction  | Comment   |
|--------------|---|---|
| End-user     |    | <ul style="list-style-type: none"> <li>- Payment fees will decrease</li> <li>- More payment options</li> <li>- New innovative banking services</li> <li>- <i>Payment more secure but more difficult</i></li> </ul>  |
| Banks        |    | <ul style="list-style-type: none"> <li>- Risk of losing contact with the end-user</li> <li>- Open its end-user data to external actors</li> <li>- Encourage new competitors</li> <li>- Additional regulation to be compliant with</li> <li>- Increase security risks since opening up</li> <li>- <i>Could generate new revenue streams</i></li> </ul> |
| AISP/PISP    |    | <ul style="list-style-type: none"> <li>- Open a new market</li> <li>- Get access to a huge base of customers</li> </ul>   |
| PSP          |    | <ul style="list-style-type: none"> <li>- New competition on their market</li> <li>- Payments more difficult</li> </ul>  |
| eCommerce    |  | <ul style="list-style-type: none"> <li>- Loss of business</li> <li>- Decrease in payment operator cost</li> </ul>   |
| Card schemes |  | <ul style="list-style-type: none"> <li>- Direct competition</li> <li>- Payments more difficult</li> <li>- <i>Fraud reduction</i> but go against 3D Secure 2</li> </ul>  |



# Bank as a Service

## Layers of BaaS platform

