



MERCHANT
PAYMENTS
ECOSYSTEM

PSD2 Acquirer Exemptions and Delegated Authentication

22.06.2020

netcetera

Introductions



Alan Moss (Moderator), VP of Marketing @ Miura Systems Ltd

Alan Moss is currently working as VP of Marketing at Miura Systems, a leading global provider of secure mobile acceptance technology. In parallel, Alan is Head of Fintech and Payments at the consulting company, BluSpecs Innovation.

Alan has over 20 years' experience in the electronic payments business, working with industry leaders such as Hypercom, Thales and Verifone, in a variety of roles from business development and product marketing to global relationship management. Alan also worked in international sales for De La Rue's security holographics and security print divisions.

Prior to working for BluSpecs, Alan was VP of Business Development at Verifone, where he was responsible for the deployment of new value-add applications and services in Europe. Whilst at Verifone, Alan was also a board member and Chairman of the General Assembly of Nexo, a leading pan-European standardization initiative promoting the interoperability of card payments. Alan holds an International MBA from Madrid's leading business school, Instituto de Empresa, as well as a bachelor's degree from the University of London.

Introductions



Roger Burkhardt

Senior Product Manager Secure Digital Payments @ Netcetera

After graduating with a Master's degree at the Institute for Computer Science at the University of Zurich, Roger began his professional career in 2006 as an account consultant in Switzerland's leading company for business information. From 2009, Roger was head of the Account Consulting department where he was responsible for advising customers on specific business processes in the area of business information. From 2014 to 2016, Roger worked for the largest debt collection company in Switzerland, as Head of Data Quality, where he was responsible for process management to ensure data quality, as well as for a fraud prevention solution specially developed for the Swiss online trade.

Since the beginning of 2017, Roger is working as Senior Product Manager at Netcetera AG in the Secure Digital Payments Division and is responsible for the product development of the company's 3-D Secure Issuer Service and of the new product eCom Exemption Advisor for Acquirers and PSP's.

Introductions



Kurt Schmid

Marketing & Innovation Director Secure Digital Payments @ Netcetera

Since 2020 Kurt Schmid is Marketing & Innovation Director Secure Digital Payments at Netcetera. Previously he has been responsible for the Digital Payment Division of Netcetera since the beginning of 2017. This resulted from the takeover of NexPERTS GmbH, an Austrian mobile payment and NFC specialist founded by Kurt Schmid, who was CEO. Previously, he was the CEO of Omnikey and Ultimaco Safeware, and has been active in the fields of smartcards and security in Germany, Austria, and Switzerland for over 25 years.

Kurt Schmid studied Business and Management Computer Science at the Johannes Kepler University in Linz, and spends his rare free time in his house and garden

An overhead view of a group of people sitting around a large wooden conference table. They are using various devices including smartphones, tablets, and a laptop. The scene is dimly lit with a blue overlay. The title 'PSD2 Acquirer Exemptions' is centered over the image.

PSD2 Acquirer Exemptions

Roger Burkhardt

netcetera

Some Facts and Figures

> 620 billion
EUR

E-Commerce revenue
in 2019

1,8 billion
EUR / per year

Credit card fraud,
in Europe

> 80%

of the fraud is from
CNP transactions

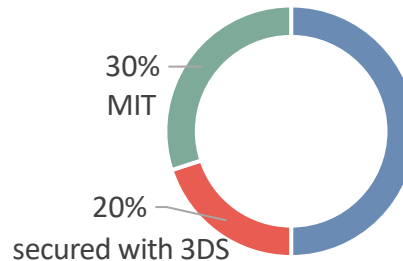
27 countries
in Europe

will have to comply
with PSD2



Strong customer authentication (SCA) and
exemptions from SCA
for frictionless user experience


E-commerce Transactions in Europe



50%

within PSD2 market to be:
authenticated via 3-D Secure or
exempted from SCA via a PSD2 exemptions

The Challenges



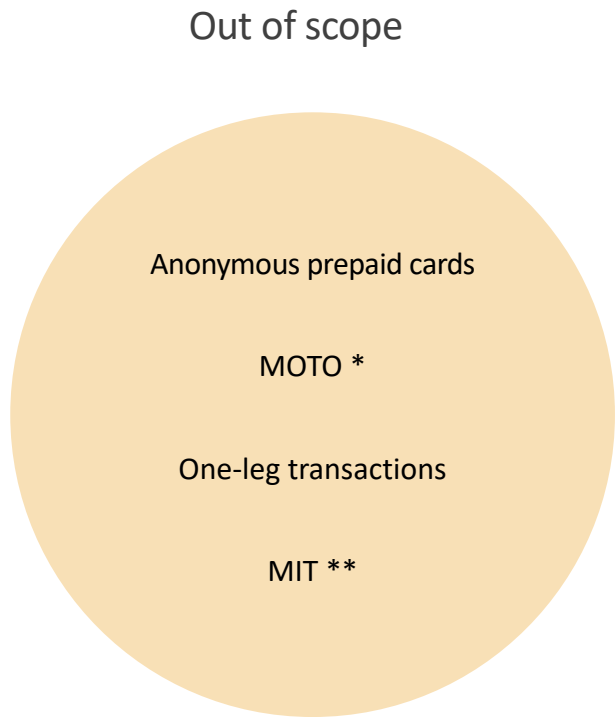
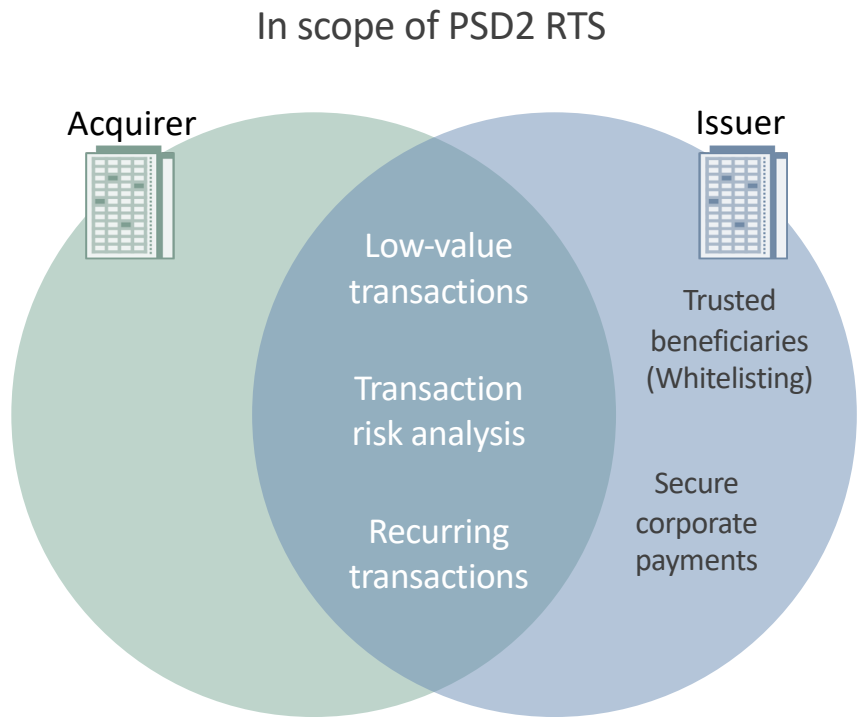
How should Acquirers and PSPs in Europe, deal with PSD2 SCA and especially with the PSD2 defined SCA exemptions?

How can Acquirers and PSPs find the right strategy?

What can Acquirers and PSPs do to maximize acceptance rates?

How is PSD2 driving innovation for new products?

Which PSD2 Exemptions can be Used by Acquirers?



* MOTO = Mail order / Telephone order

** MIT = Merchant initiated transaction

Low Value Transactions

1

Transaction amount $\leq 30\text{€}$

AND

2

Σ (Transaction amounts since last SCA) $\leq 100\text{€}$

OR

N° (Transactions since last SCA) ≤ 5

Acquirers cannot correctly count the number of consecutive low value transactions
nor the cumulative amount since the last SCA.

This can only be checked by the issuer during payment authorization.

Transaction Risk Analysis (TRA)

1

Low level of risk
Risk assessment is mandatory!

2

Transaction amount \leq ETV *
(based on the Acquirer's fraud rate)

* ETV = Exemption threshold value

ETV (in €)	Reference fraud rate *
> 500	Not applicable for TRA
$250 \leq 500$	1 bps = 0.01% (1 out of 10.000)
$100 \leq 250$	6 bps = 0.06% (6 out of 10.000)
≤ 100	13 bps = 0.13% (13 out of 10.000)

* for remote electronic card-based payments

Fraud reporting to National Competence Authority

Recurring Transactions

Same amount + Same payee
as the initial transaction

MIT processing applied for different amounts

* MIT = Merchant Initiated Transaction

Complex implementation logic

Defining decision making rules for authentication of subsequent transaction

The Goal: One-click payments

Enabling the frictionless flow with Acquirer's Exemptions

- **Low Value Transactions**
- **Transaction Risk Analysis**
- **Recurring transactions**
- Delegated Authentication
(SCA already performed)

Taking the Right Decision!

Acquirers / PSPs should define an exemption strategy to be able to decide whether a transaction should be sent..

01

with an Acquirer's exemption directly to authorization or

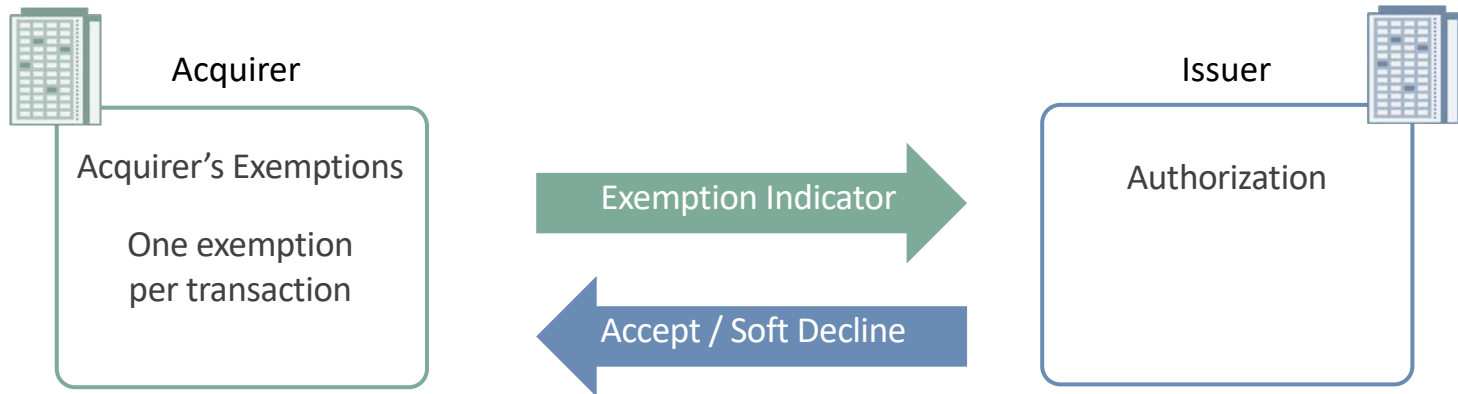
02

with an Acquirer's exemption to 3DS authentication (through the 3DS Requestor Challenge Indicator)

03

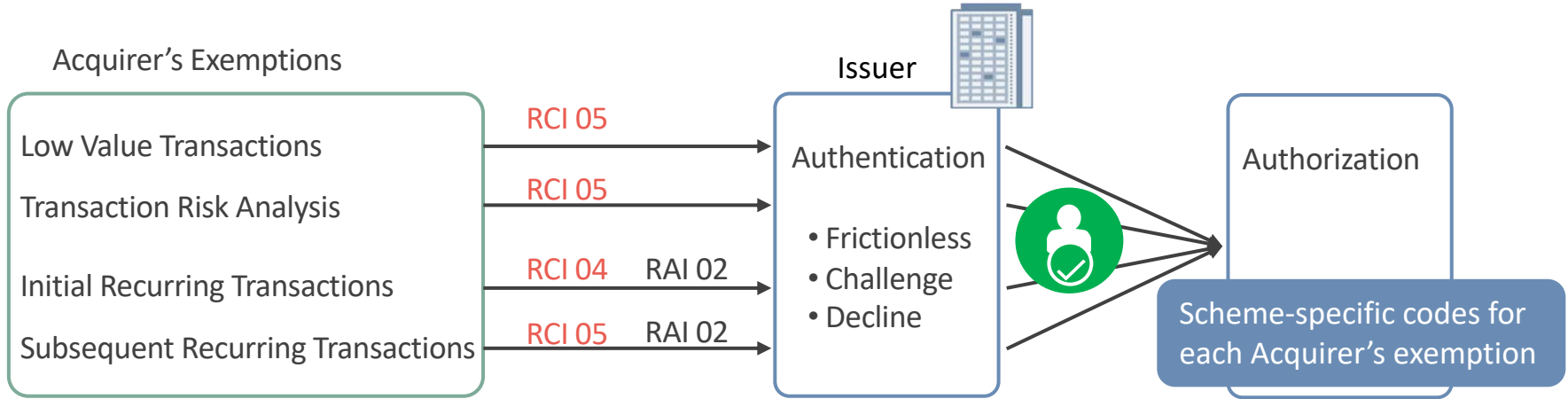
without an Acquirer's exemption to 3DS authentication

Direct Authorization With Acquirer's Exemption



When a transaction is soft declined, it must go to 3DS, even in case another exemption could be applied
The schemes recommend Issuers to not systematically decline authorizations without authentications

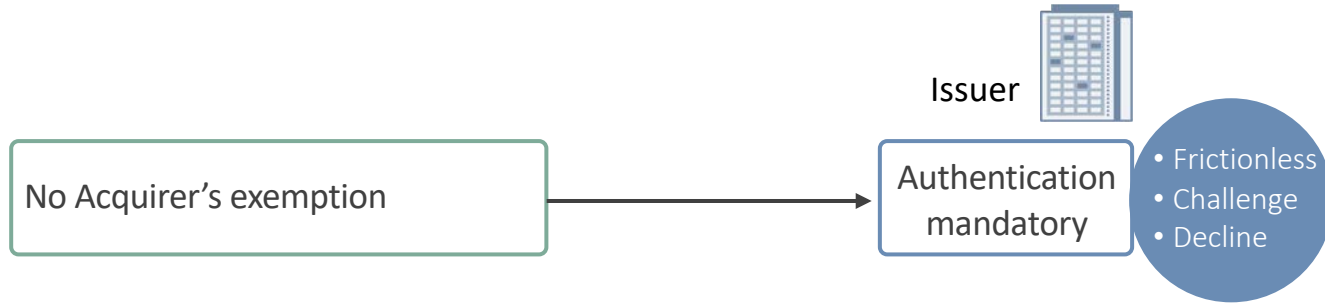
3-D Secure Authentication With Acquirer's Exemption



Higher probability for successful authorization compared to direct authorization

Issuers cannot differentiate between Low-Value and TRA Acquirer's exemption in the authentication, which is only possible in authorization

3-D Secure Authentication Without Acquirer's Exemption



Liability Without 3DS Authentication

Acquirer's Exemption	Low Value Transactions	Transaction Risk Analysis	Initial Recurring Transactions	Subsequent Recurring Transactions
Authentication	None	None	None	None
Authorization	Accept Acquirer's exemption + check counters	Accept Acquirer's exemption	Not compliant	Accept Acquirer's exemption
Liability	Acquirer	Acquirer	Acquirer	Acquirer

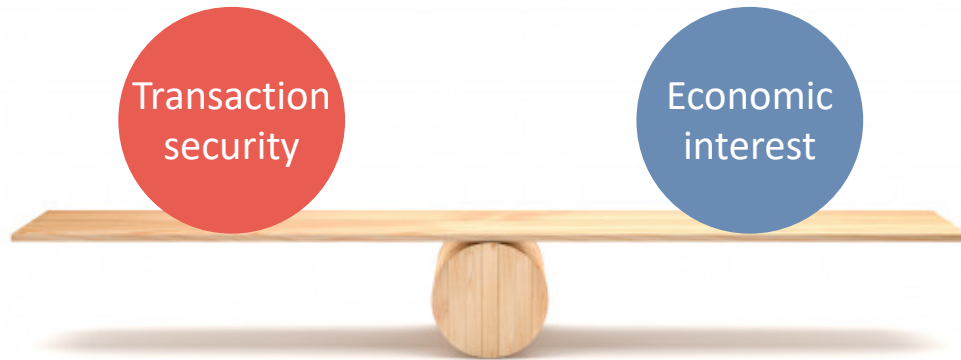
Liability With 3DS Authentication

Acquirer's Exemption	Low Value Transactions	Transaction Risk Analysis	Initial Recurring Transactions	Subsequent Recurring Transactions
Authentication	Accept Acquirer's exemption	Accept Acquirer's exemption	Challenge	Accept Acquirer's exemption
Authorization	Accept Acquirer's exemption + check counters	Accept Acquirer's exemption	Accept	Accept Acquirer's exemption
Liability	Acquirer	Acquirer	Issuer	Acquirer

Summary

Finding the right balance...

... based on risk assessment and exemption possibilities



How to Find the Right Balance?

Continuous transaction and fraud data analytics

Identification of possibly exempted transactions (PSD2, DA, Out of scope, MIT)

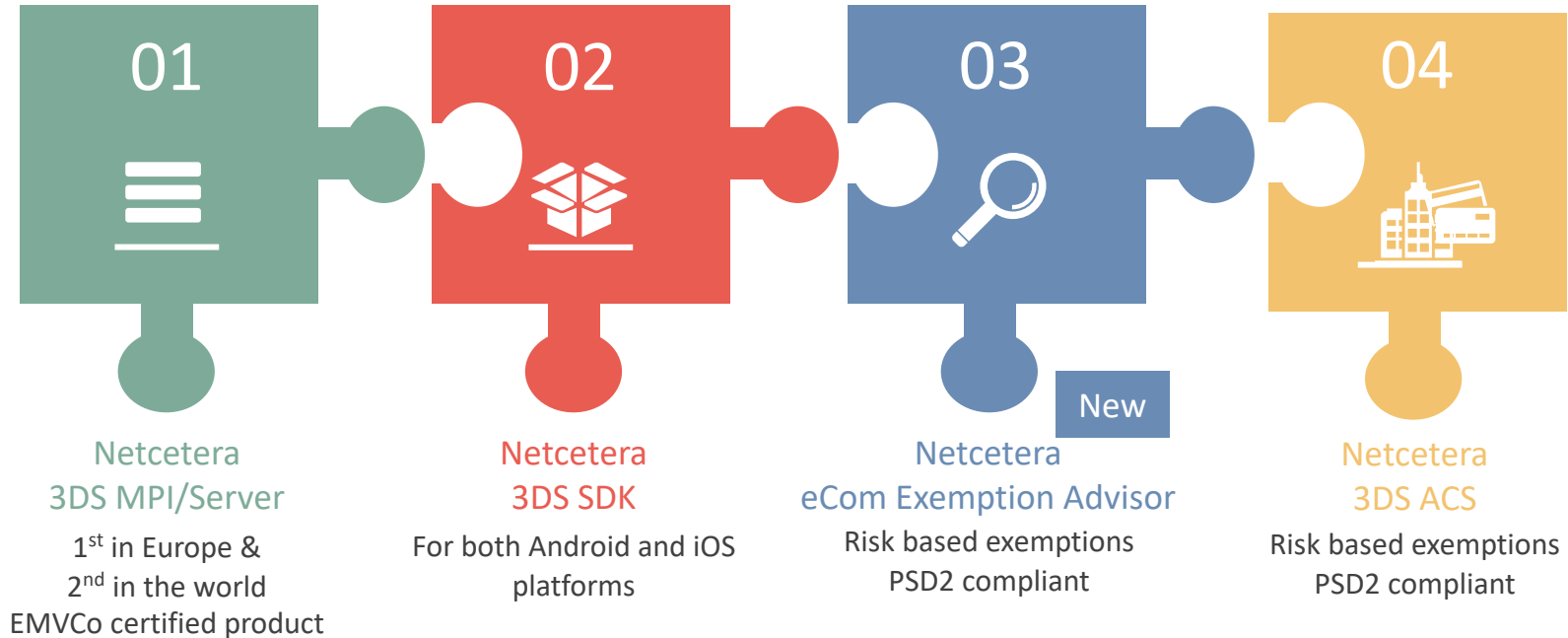
Identification of fraud patterns and high risk transactions

Continuous optimization of the risk management

Acquirers: take the right decision: exemption or 3DS authentication

Issuers: take the right decision: exemption, SCA or declining

How Does Netcetera Support You?



New: Netcetera eCom Exemption Advisor

for the acquirers / PSPs

eCom Exemption Advisor

**Exempt the transaction or
proceed with 3DS authentication**

PSD2 exemptions

Transaction Risk Analysis
Low-value-payments
Recurring payments

SCA out-of-scope exemption

One-Leg-Check

Delegated authentication

For more info contact: 3dss@netcetera.com

Helps you make
the right decision

Flexible model

Customer's choice
of exemptions

24x7 operational

Real time
performance

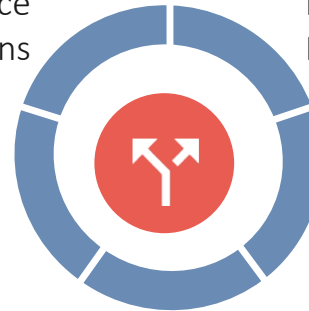
Risk assessment

Partner with Inform
RiskShield solution

Operated by Netcetera

Highly secured data centers
PSI-DSS certified

Fast Integration



A close-up photograph of a person's hands. The left hand is holding a smartphone, and the right hand is holding a credit card. The background shows a laptop keyboard and a person's arm in a blue shirt. The scene is dimly lit, with a warm light source from the right.

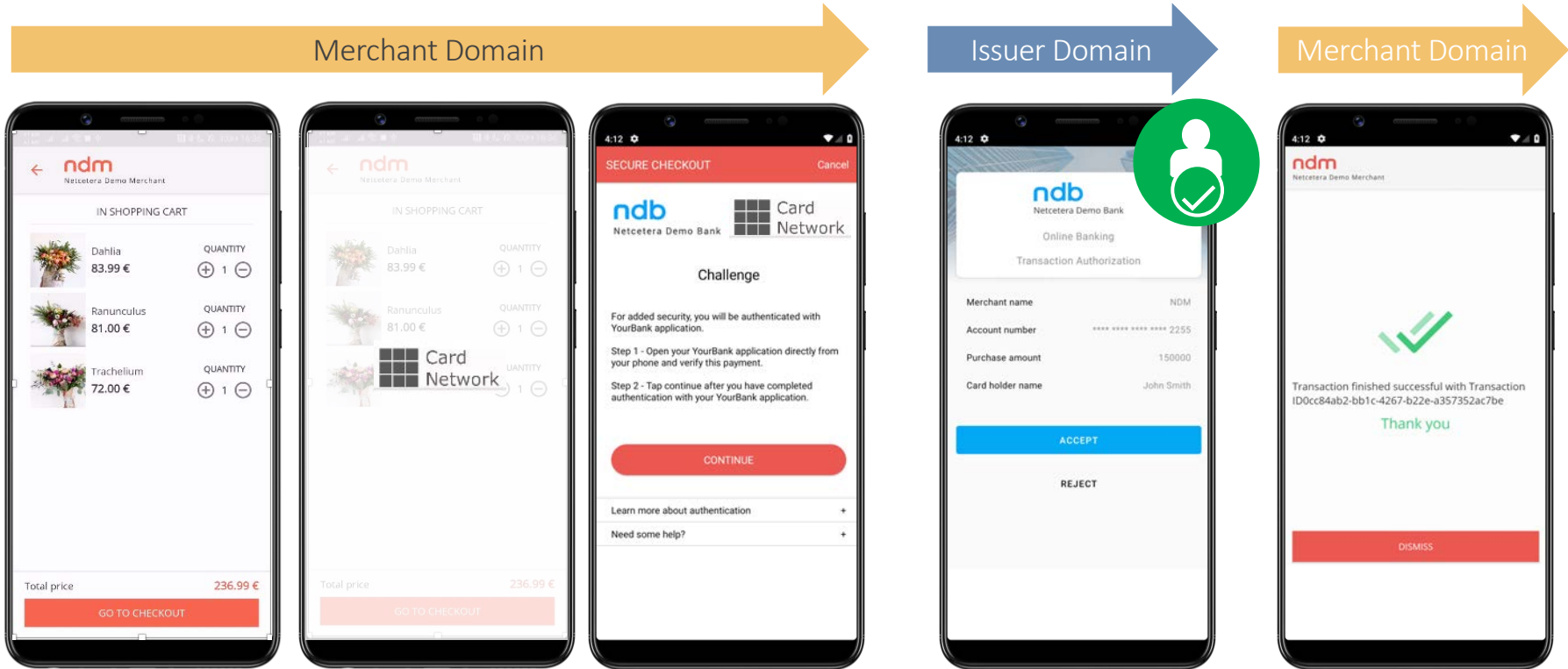
Delegating Authentication

More details in our Payment News & Trends webinar on Delegating Authentication see [trends.Netcetera.com](https://trends.netcetera.com)

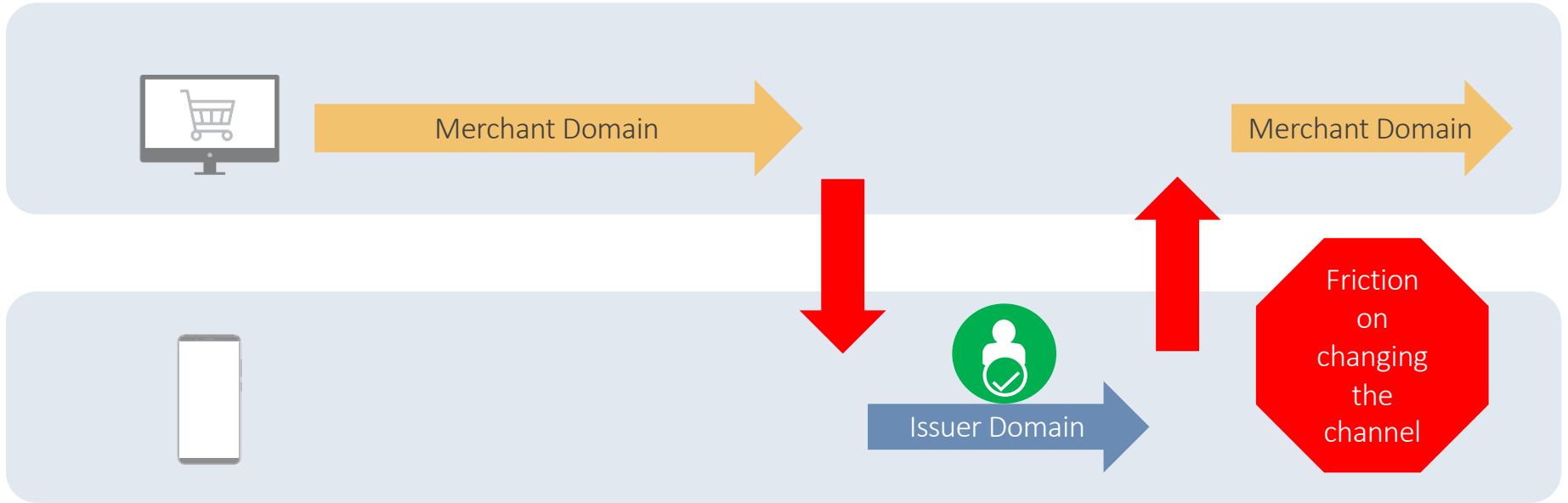
Kurt Schmid

netcetera

How does it look like to the consumer (in best case)



More Problematic When Shopping on the Web



What are the Problems With the 3DS Flow?

- 24%** Abandonment & decline rate when 3DS (1.0) is used
- 17%** Decline rate when 3DS is not used
- 1 in 4** Customers abandon cart due to long /complicated checkout
- 4-10** Times higher fraud rate of CNP compared to CP

RESULTING IN
FRICTION

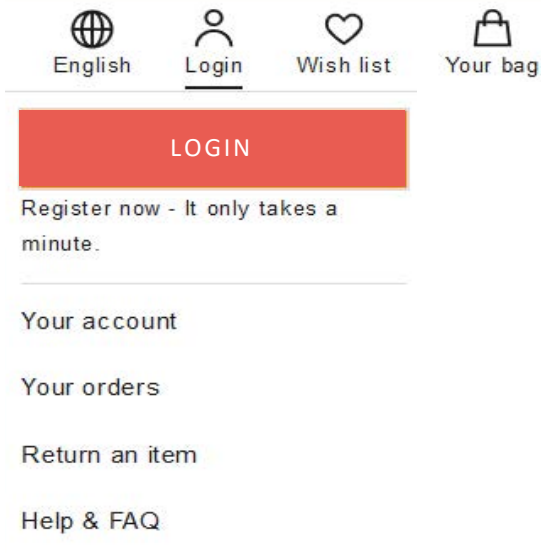


Delegation (to Merchant)



Many Merchants Already Knowing Their Customers

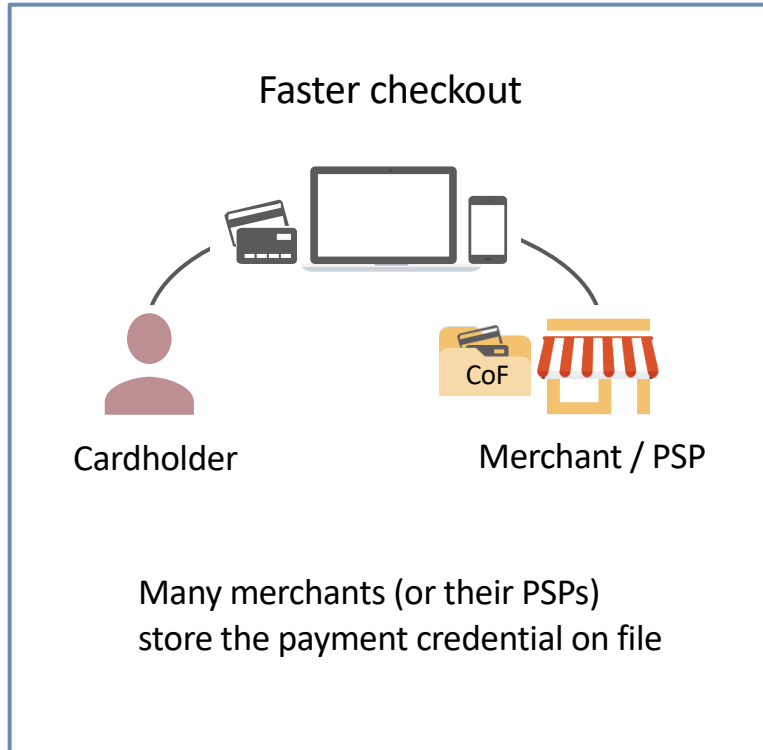
All big e-Commerce merchants already know their customers and have mechanism to authenticate them



- Better support across channels
- Easier consecutive shopping
- Better overview and tracing
- Wish lists and more

On mobile devices,
the use of biometrics is already standard and
eases the authentication process

Card On File (COF)



Advantages when using **network tokenization**
(details see last webinar)

- Better conversion rates
- Better UX
- Support for notifications from issuer to merchant

Details in our Payment News & Trends webinar on
Tokenization see [trends.Netcetera.com](https://trends.netcetera.com)

Good Reasons for Delegation

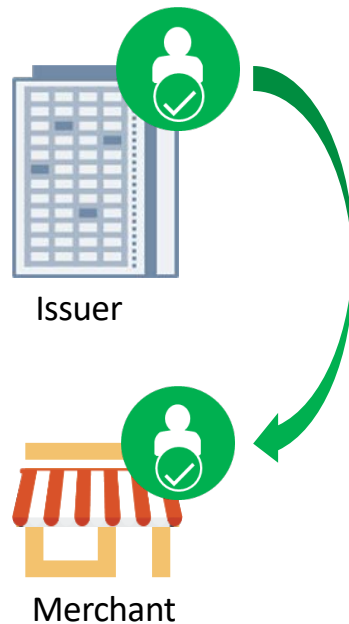
“Delegating authentication (to merchants)”

Off-loading the authentication from issuers

Perform authentication already at the merchants sphere

Benefit: seamless/ frictionless customer experience

However technically this “*merchant authentication*” is not a delegation of authentication services rather than a performing the authentication services by another party (issuers could see this differently)



Authentication at the Merchant: Key Questions



- 1 What is the method / standard for authentication?
- 2 What is needed to be PSD2 compliant?
- 3 How is the authentication confirmed to the issuer?
- 4 What is the ecosystem for this? How does it scale?
- 5 Where is the liability?
- 6 What do I need to do as merchant / PSP / acquirer / issuer?

What is the Standard / Support for Authentication?

This is specified by 3DS Standards
(and detailed by schemes)



<https://fidoalliance.org/>

Defines standard
for authentication

supports

OEMs / key software players



Networks



E.g. Apple biometric authenticators (FaceID..),
Microsoft Hello on PCs, Android...

FIDO2 is also supported by leading web browsers Google Chrome, Mozilla Firefox, Microsoft Edge (with preview support by Apple Safari). Android has also been FIDO2 Certified, allowing mobile apps and websites to leverage FIDO standards on over a billion devices supporting Android 7.0+.

What is Needed to be PSD2 Compliant?

Requirement RTS
for PSD2 SCA:

The authentication shall be based on two or more elements which are categorised as knowledge, possession and inherence and shall result in the generation of an authentication code

How does FIDO meet
the requirements:

To authenticate with FIDO, the Payment Service User (PSU) must possess a FIDO authenticator that is either integrated in a general purpose device (e.g. Smartphone, Laptop, ...) or in a separate device (e.g. Security Key, smart card...).

As seen in chapter 2 of this document, possession of such a FIDO authenticator satisfies the first of the two elements required to authenticate the PSU.

The second element required to authenticate the PSU consists in:

- For U2F, a password sent on-line and verified by the server
- For UAF and FIDO2, an inherence (biometric) factor or knowledge (PIN) factor verified locally by the FIDO authenticator

The signed response, created by the authenticator and returned to the ASPSP, constitutes the authentication code mandated by the RTS.

FIDO and RTS for PSD2: https://fidoalliance.org/how_fido_meets_the_rts_requirements/

How is the Authentication Confirmed to the Issuer?

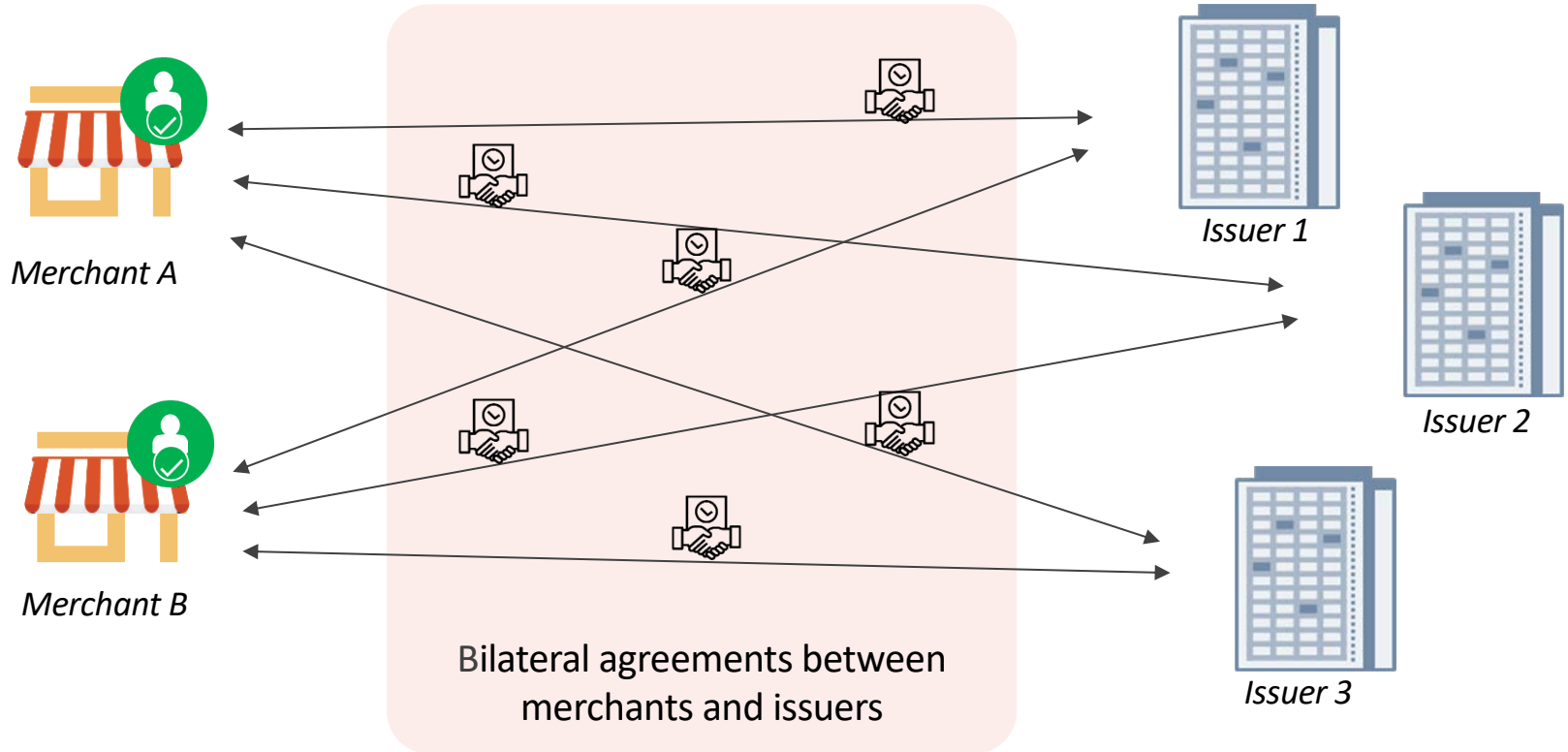
Transmit
“already delegated state
to the ACS of the issuer”



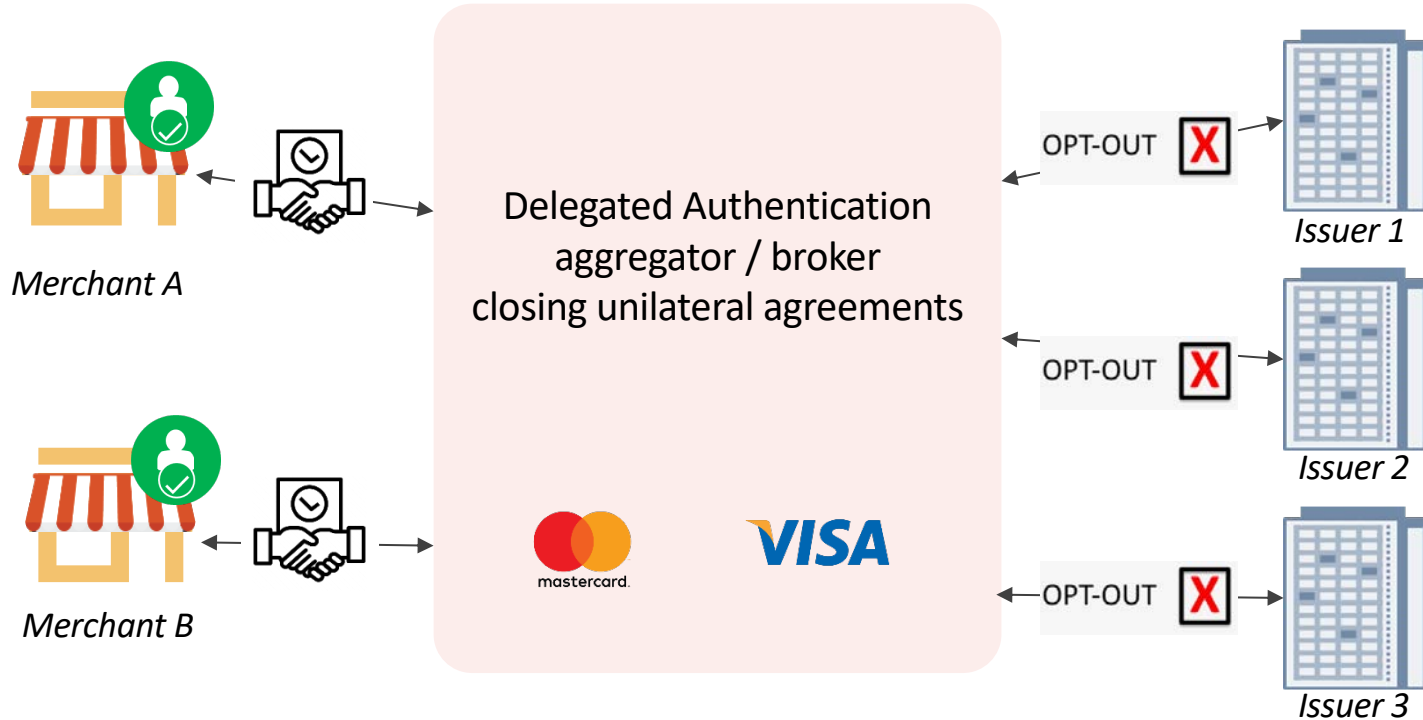
Available
partially with 3DS 2.1 and
fully with 3DS 2.2 protocol

	EMV 3DS 2.1 – PSD2 Mastercard Message Extension (AN 2758 —Announcing the New EMV 3DS 2.1 Mastercard Message Extension in EEA Countries)	EMV 3DS 2.2
Feature		
SCA Exemption (in ARes and RReq only)	PSD2 Mastercard Message Extension AReq Field 1 = 3DS Requestor Challenge Indicator 05 = No challenge requested (transactional risk analysis is already performed). 05 will be used for the following Acquirer exemptions: low-value payment, TRA, recurring payment AND MIT (refer to section on Merchant-Initiated Transactions) 07 = No challenge requested (strong consumer authentication is already performed under Issuer delegation). <i>AN 2714—Authentication Express—an Authentication Program Enabling Easy and Secure Multi-Lateral SCA Delegation</i> announces the Mastercard SCA delegation service (Authentication Express) availability. For both values “05” and “07”, the ARes will include a transStatus = “N” and transStatusReason = “81”.	Already supported in specs Field three DS Requestor Challenge Ind = Same values as in previous column. For both values “05” and “07”, the ARes will include a transStatus = “I”.

Relation Between Merchants and Issuers



Relation Between Merchants and Issuers



The Schemes and Delegated Authentication

Mastercard and VISA have introduced own “DA broker” programs:



Visa Delegated Authentication Program Implementation Guide

November 2019

Version 1.2
6th November 2019

VISA

Where is the Liability?

No agreement between merchant and issuer or broker:

A merchant can flag a transaction as
“I did authenticate the consumer” and
the issuer may refrain from challenging the consumer;
anyhow it is up to the issuer to decide to
request challenge or allow the flow frictionless

Liability is with issuer once to decide to request challenge,
otherwise it is with merchant

Bilateral agreement between merchant and issuer:

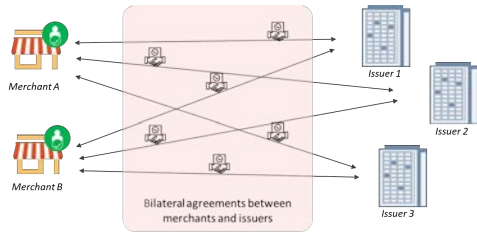
Depending on the agreement

A merchant sign-ups to the DA programs from Mastercard / VISA:

Liability is with the issuer;
however issuer may opt out from the program for BIN ranges



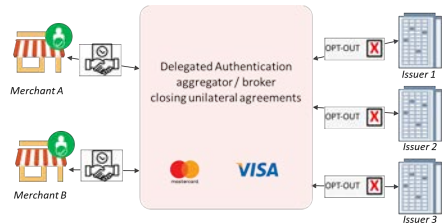
What do I Need to do as Merchant / PSP?



Legal agreements with Issuers

Technical implementation / Test

Roll out



Legal agreements with brokers

Technical implementation

Certification / Test

Roll out

Functional Epics (for a Merchant / PSP)

1

User Registration / Identification

- Recommended:
3DS NPI Authentication, but also 3DS Payment flow initially needed

2

Device Authenticator enrollment

- Device Discovery
(which Authenticators are available)
- Enrollment of Authenticator

3

Binding of consumer card and authenticator with DA broker

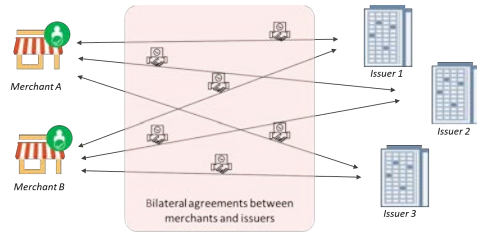
- Prerequisite is 1. and 2.
- Enroll the delegation at the broker service or with the issuer

4

Transacting

- Use Authenticator to validate consumer
- Send FIDO data to broker service or issuer

What do I Need to do as Issuer?

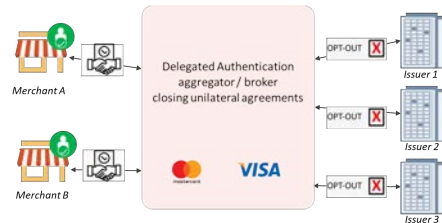


Bilateral legal agreement(s)

Technical Implementation

Onboard merchant

Roll out



No opt out

Technical adaptations (3DS 2.2)

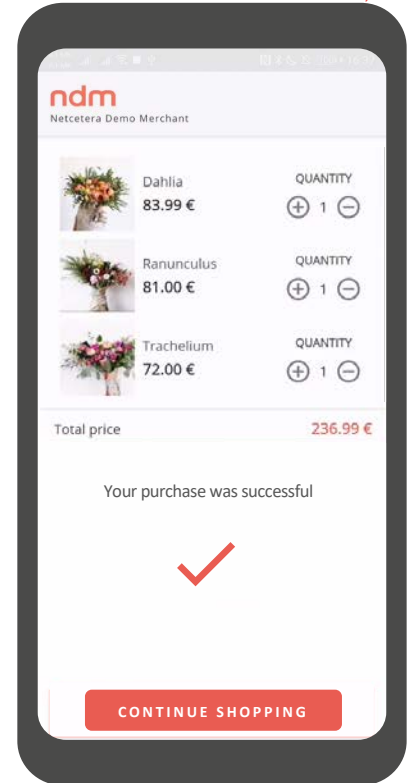
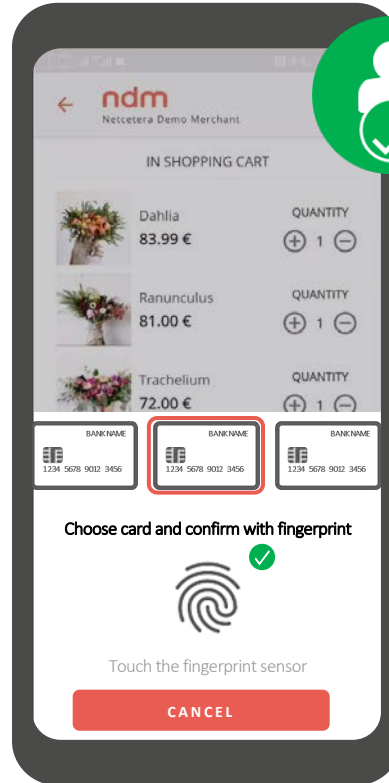
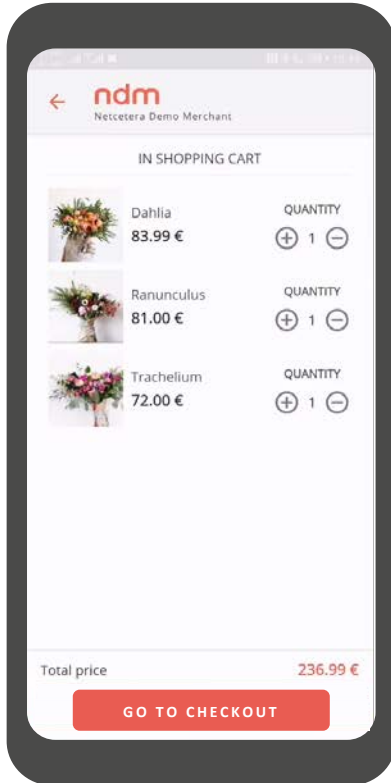
Roll out

Consumer experience

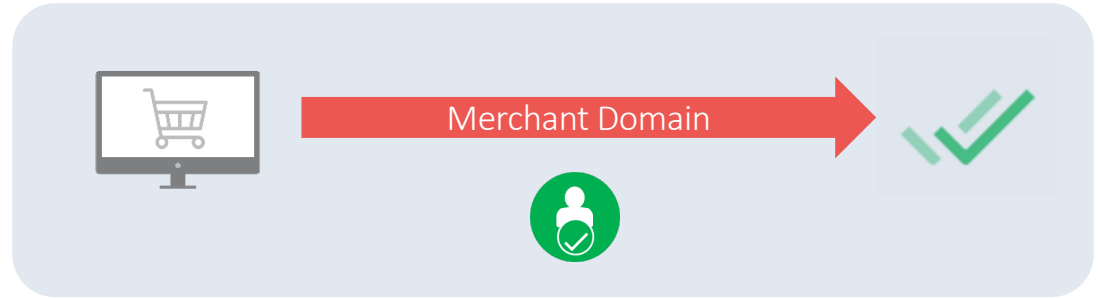
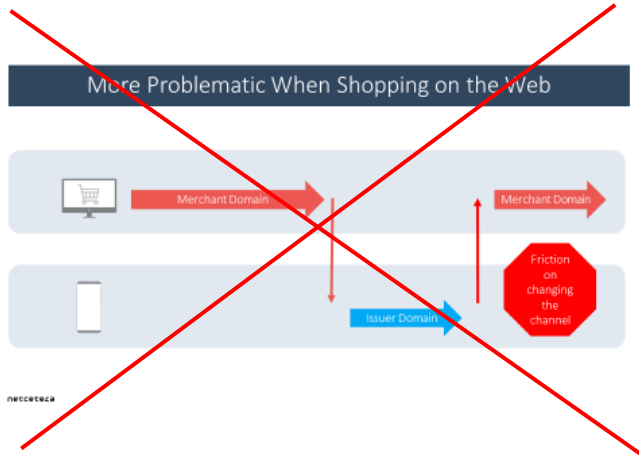


How Does it Look Like to the Consumer

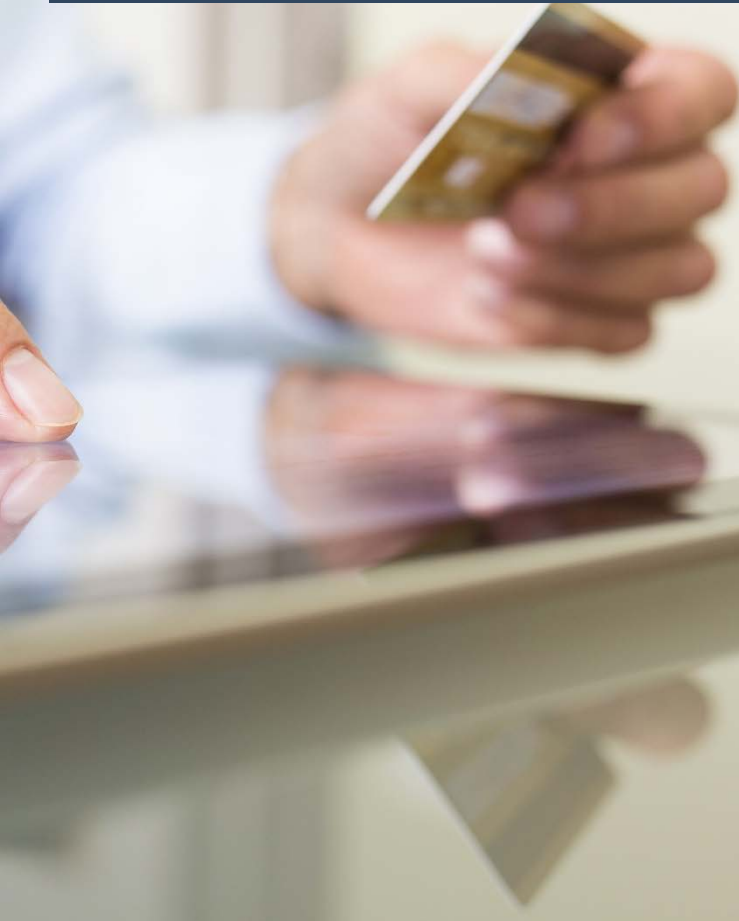
Merchant Domain



When Shopping on the Web



Key Findings – Summary



- Delegated Authentication can deliver the PSD2 compliant one click checkout
- As many customer are already known by their merchants, it is a logical next step to implement this
- Although it looks technically ambitious, by choosing a right DA service provider the implementation can be quick when using a broker model
- Longer term key merchants will close agreements with issuers as well

Contact us

Roger Burkhardt



Senior Product Manager Secure Digital Payment
Roger.Burkhardt@netcetera.com

Connect on [LinkedIn](#)



Kurt Schmid



Managing Partner Secure Digital Payment
Kurt.Schmid@netcetera.com

Connect on [LinkedIn](#)



Q&A

Please raise your hand or
use the question section



THANK YOU FOR ATTENDING!

netcetera



MERCHANT
PAYMENTS
ECOSYSTEM

Recording and presentation will be provided via e-mail
and all videos are available on trends.netcetera.com