



EXEX - 8th May 2019, Riga.
"Secure Customer Journey in E-Commerce"

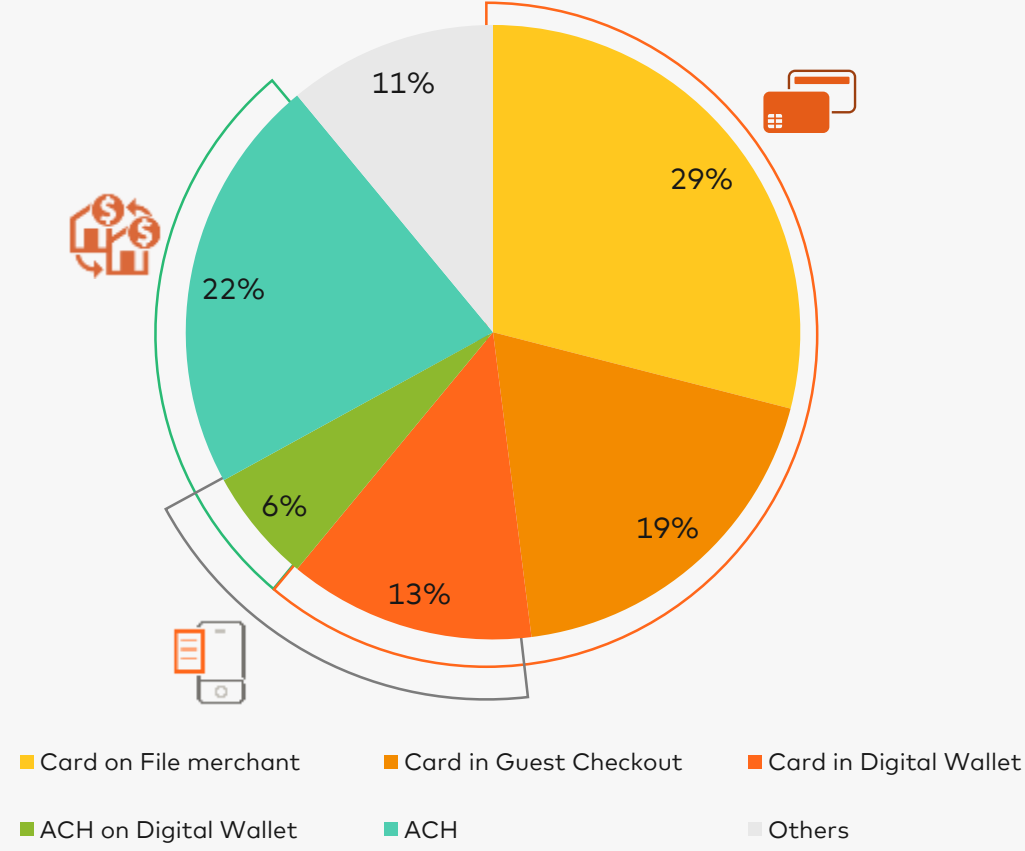
1. Landscape
2. MDES tokenization for Merchants.
3. Secure Remote Commerce, SRC, Overview
4. Strong Customer Authentication, SCA mandate September 2019.

Björn Salomon-Sörensen, Director Mastercard.

Cards are the most used payment tool for e-commerce but needs to act to make card payment compliant and competitive in PSD2 world

ECOMMERCE SPEND BY PAYMENT USE CASE

Europe 2017, 100% = 864B€



CHALLENGES FOR CARDS IN ECOMMERCE

24% Abandonment + Decline rate **when 3DS is used**

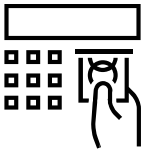




17% Decline rate **when 3DS is not used**

10x Fraud rate of ecom Vs card present

? Consumers tend to forget where they registered their card. So it's a problem to keep track.

We envisage a world with **no friction** and **no fraud** in **any commerce use case**

CHANNELS /
PAYMENTS
USE CASES

PHYSICAL COMMERCE	DIGITAL COMMERCE			
 <p>In-store POS <i>(M-Chip)</i></p>	 <p>Guest Checkout <i>(SRC)</i></p>	 <p>Credential-on-File <i>(M4M)</i></p>	 <p>Commerce Platforms <i>(M4C)</i></p>	 <p>Devices <i>(DSRP)</i></p>





MDES for Merchants

Creating a more secure and convenient ecommerce experience with tokenization from Mastercard Digital Enablement Service.

Introduction for Financial Institutions



Tokenization is the process by which the original card number is replaced with a surrogate value called a "token."

MDES (Mastercard Digital Enablement Service) for Merchants delivers tokens with enhanced capabilities:



Original Card Data

Traditional 16-digit card number & data



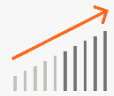
Tokenization

An alternative number replaces the PAN and is mapped to the funding account to manage account lifecycle

Digitization

Tokenized card details, associated data and card art delivered onto the merchant server

M4M tokens provide several benefits over standard Primary Account Numbers (PANs)



Better Approval Rates

- **Reduces card lifecycle related declines** by keeping card information up to date
- Mastercard tokens **provide issuers with additional visibility** for fraud scoring to **increase approval rates**



Interoperability

- Tokens can be handled by issuers, acquirers and PSPs just **like normal PANs** across the world



Enhanced Security

- **Tokenization enhances security**, M4M tokens are merchant specific reducing the risk of data breach
- MDES is **validating that the transaction is coming from the right merchant** through the use of cryptographic data



Improved User Experience

- **Card-on-file payments are not disrupted** even when cards are updated or expire
- **Merchants receive issuer card art** assets to display to consumers

Introducing Secure Remote Commerce

Secure Remote Commerce is a global standard issued by EMVCo designed to create a digital checkout experience that delivers the security, convenience, and control consumers experience for **guest checkout** in e-commerce.

Presented together by the payment networks, Secure Remote Commerce will enable scale across all devices, operating systems, apps and browsers.



CONSUMER BENEFITS



Enjoy a predictable, simple and secure checkout experience.



Secure storage of payment information all in one place



Consistent checkout experience completed in just a few clicks without static passwords*



Uninterrupted recurring payments with automatic credential updates



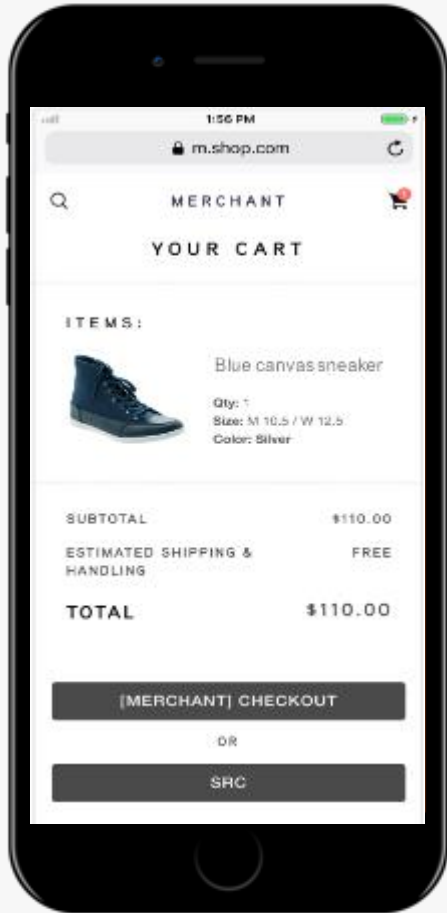
Visibility and control over where payment credentials are stored

* For registered SRC users

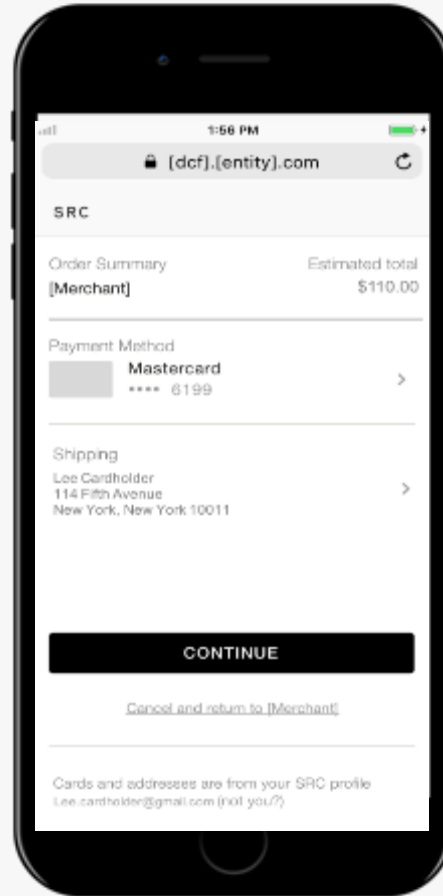


Consumer is recognized: Enrolled user transacting on a device they trust

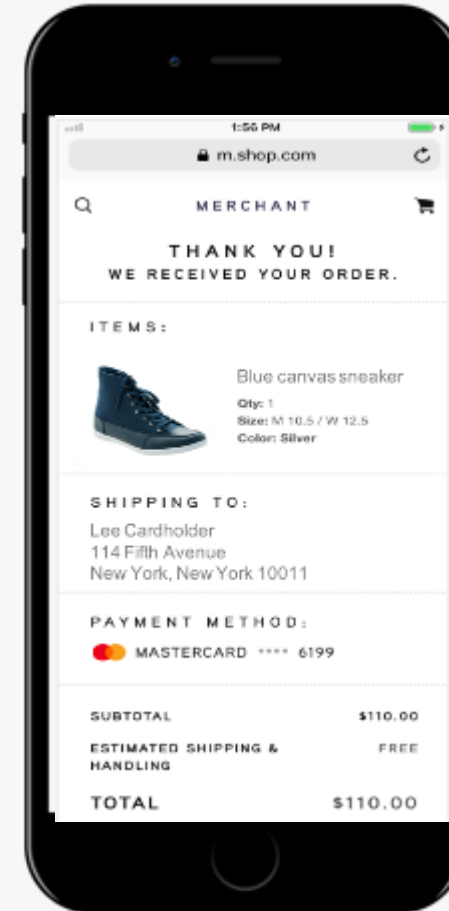
Merchant



SRC



Merchant



Key benefits

- ✔ **Better User Experience** with streamlined and consistent password-less guest checkout
- ✔ Potential for **higher approval rates** and **decreased fraud** with tokenization, cryptography and strong authentication
- ✔ **Reduced checkout friction** with fast enrollment of consumers and potential for frictionless authentication
- ✔ **Reduce effort** required to integrate and maintain multiple buttons through standardized checkout
- ✔ **Deeper consumer engagement** with issuer card art at checkout and value added solutions



The Strong Customer Authentication legislation: The main objectives of this new regulation is to reduce fraud while minimizing the impact on customer experience.

1

To reduce fraud...

Ecommerce card fraud losses are a major problem in Europe¹



€1.8bn

Out of all card fraud in Europe, CNP fraud is the largest³



75%

Card-not-present (CNP) transactions are more likely to be declined²

Digital



15-20%

vs.

Physical



2-3%

2

...while minimising the impact on customer experience

Static passwords & authentication methods are outdated

20-25%
online purchases
in Europe
are abandoned
before completion⁴

False declines impact cardholders' trust

1/3
after being
falsely declined consumers
either abandoned their
card or used it less⁵

Consumers prefer faster processes and show readiness for new solutions (e.g. biometrics)

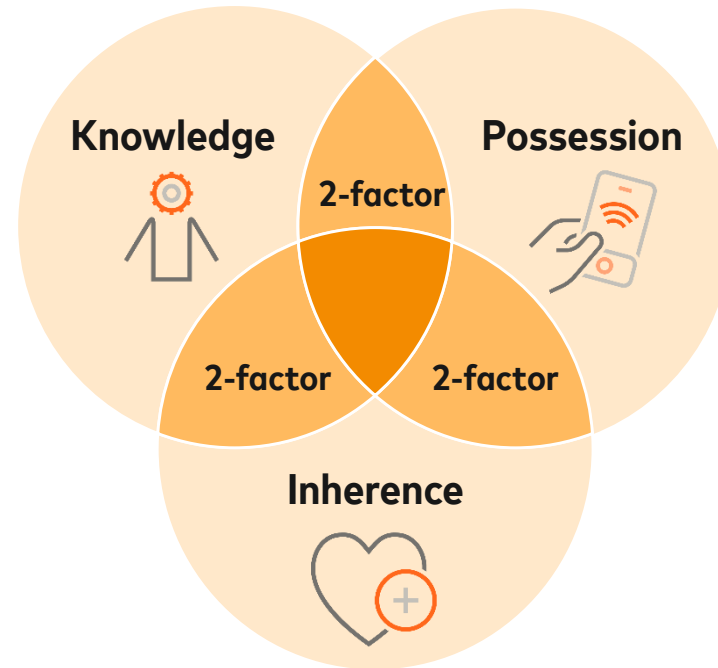
58%
of interviewees
positively
evaluate biometric
solutions⁶

The Strong Customer Authentication legislation is redefining the security standard for e-com payments

SCOPE

- On-line / **remote payments** (incl. card on file)
- **In store electronic** payments (e.g. mobile/contactless)

KEY PRINCIPLE



Main EXEMPTIONS (for low risk transactions)

- Remote transactions **up to EUR 30** (for 5 consecutive transactions, or total of EUR 100)
- Remote transactions between **EUR 30** and **EUR 500** provided **RBA is applied** by the issuer or the acquirer and **their fraud rates are under specific thresholds**
- Remote transactions to **white lists of trusted beneficiaries and recurring transactions**

Merchants need to liaise with Acquirers and Issuers to enable best payment experience for their cardholders while ensuring compliance with the new regulation

Increase Transparency

- Enrol into EMV 3DS
- Enrich authentication message
- Encourage issuers to maximise exemptions

Drive Loyalty

- Promote whitelisting solutions
Leverage recurring transactions and MITs

Enablers:



Communications



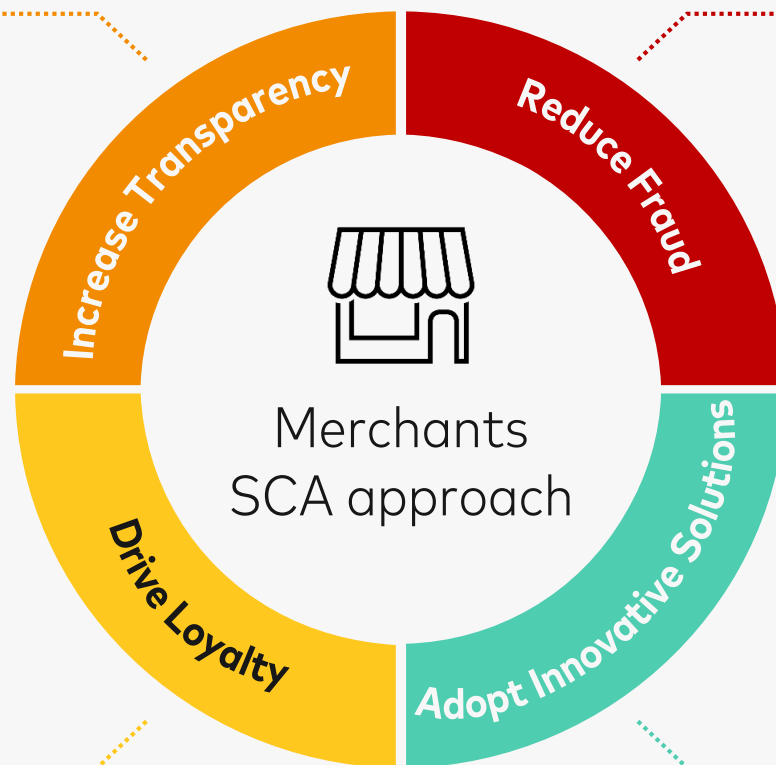
Technology



Partnerships



Cybersecurity



Reduce Fraud

- Implement new solutions (e.g. tokenization, fraud engines)
- Collaborate with acquirers (e.g. bring down fraud levels and leverage TRA exemptions)

Adopt Innovative Solutions

- Implement or adopt **biometric solutions**
- Assess **solutions available in the market**

Thank you very much!

