# Delegated authentication: simplifying the e-commerce checkout process

**When it comes to e-commerce and payments, the biggest concern is cart abandonment at the checkout. However, tokenization and Strong Customer Authentication can prevent it.**

The "new normal" has been a major accelerator in the shift to digital for most of us – how we work, how we connect with friends, and definitely how we shop. Furthermore, because of new behavior in shopping, many brick-and-mortar retailers are shifting from a pure physical business model and going online.

Jukka Yliuntinen, Digital Payments champion at Giesecke+Devrient (G+D) explains how to be a winner in this shift, and leverage on your online business when it comes to pay.

The changes that the e-commerce industry will have to embrace to adapt to the "new normal", for merchants, it will be essential to rapidly expand their omnichannel capabilities – which will bridge payments in any environment, physical or digital.

On the e-commerce side, we should see greater adoption of the kind of 'one-click' payment solutions. This frictionless payment allows consumers to shop in a seamless way. When it comes to payment and 'easy buying', this is driven by customers' expectations both on how easy it is and on how secure one platform from another is to buy from. They have to feel safe when buying.

Also, there are different types of challenges specific to customer experience retailers are facing when it comes to paying online. And this is a hot topic as merchants depend on the usability the card issuers are offering, in order to enable a nice checkout experience.

Online a customer can easily pick, compare, and choose what to buy, and also use different methods to do so. And bam, the checkout doesn't convert! The big pain here is authenticating the consumer enabled typically by the card issuing bank.

At the checkout, the consumer faces two types of authentication: first when logging in and authenticating herself as a user of the merchant's app, and then for a second time at the checkout, with authenticating herself as owner of a card. This gives friction that leads to cart abandonment.

But there are solutions merchants can leverage upon to balance compliance, costs, and UX such as a card-on-file solution (CoF) like G+D's Convego® CloudPay eCOM solution supporting network tokenization. With this solution, merchants can offer secure payments without having to store sensitive customer data, avoiding the need for costly risk management tools, and removing the risk of data security breaches and cyber threats. Instead a merchant can stay ahead of the competition by focusing on the core business and at the same time offer a state-of-the-art and convenient customer experience when it comes to fulfilling the payments at the checkout.

This is done thanks to optimized Card Lifecycle Management where the network token is decoupled from the funding card for automatic renewals, and as a result there is no need for the customer nor the merchant to update any card data if as/when cards expire as this is done automatically. Network tokenization offers significant benefits over proprietary solutions:

- Higher security as the tokenization goes through a Token Service Provider and each transaction has a cryptogram;
- Network Tokenization covers a variety of use cases such as in-car payments, in-app, and mobile e-commerce payments;
- Convego CloudPay eCOM offers multiple payment brands and network tokenization with a single integration – scalability and convenience!
- Automatic token refresh at card renewal, no interruption to scheduled payments and no discontinuation of service.

Combine CoF network tokenization with embedded Strong Customer Authentication (SCA), the customer experience will be even more satisfying at the checkout. If SCA is already done when the consumer is logging in to the merchant's app, the issuer can rely on that authentication and won't ask for another one for processing the TRX, fastening up the payment process making it seamless. We call this delegated authentication.

In an nutshell, the winning concept with network tokenization is the fact that the funding PAN is not stored by the merchant or PSP, each transaction is secured by a unique cryptogram, the network tokenization provides a unified global infrastructure and domain controls, the payment execution is secure by design with technology you can trust.

The European Banking Authority (EBA) was requested to grant an 'at least additional six months' for enforcing SCA due to COVID-19. However, the European Commission (EC) would not support any further delays of the full application of SCA (except for the UK and France).

So what steps do merchants need to take now to ensure compliance with SCA in time for the enforcement deadline (31 December 2020)? Well, the payment schemes and the regulators have invested a lot in securing the customers and not only online merchants. This enables the e-commerce to keep on growing with an impact on the development of online payments.

The challenge in developing new ways to pay online needs to take the schemes' and regulatory requirements into account, but also has to provide a technology that caters the customers' wanting a smooth payment experience. As technology is rapidly developing there is a lot of investment needed to stay on top.

From a security aspect, it is hard to do all of this alone. Even if you have the resources, you always have to plug into a network of systems for coherent E2E secure payment. I call this system-wide security which is the thing to ensure you are up to date. To have a vendor connecting the dots in this network, managing it all, merchants can really benefit and focus on their core business: selling goods.

And e-commerce is booming! The growth of online commerce has accelerated and will continue to do so, especially as markets, such as those in Southern Europe, close the gap with more advanced Northern European or Anglo-Saxon economies and China.

The main driver behind e-commerce - corona or no corona – is still internet providing information and access to almost everything, with most companies using the internet to offer their services online.  And after years of promise and variable customer adoption to digitalization, the new-normal might be the last push enabling digital payments technologies to finally come into their own.

At G+D we see great opportunities for e-commerce to leverage on our tokenization and authentication solutions already in use online and offline, mobile, and physical. As a leading global provider of physical and digital authentication and payment solutions, with unique end-to-end offerings along the whole physical, electronic, and digital payment cycle, our solutions are securing billions of consumers in their daily life when it comes to pay.

### 25-40 year olds
Digital natives change the way to pay: With the emergence of new financial service providers, the so called Millennials are changing the way they pay for items online or in stores.

### Tokenization booming to 95%
In 2022 the amount of tokenized e-commerce payments will hit 95%. Tokenization refers to the process whereby something with low, or no, intrinsic value replaces something with high value payment, hence secure and easy to use!
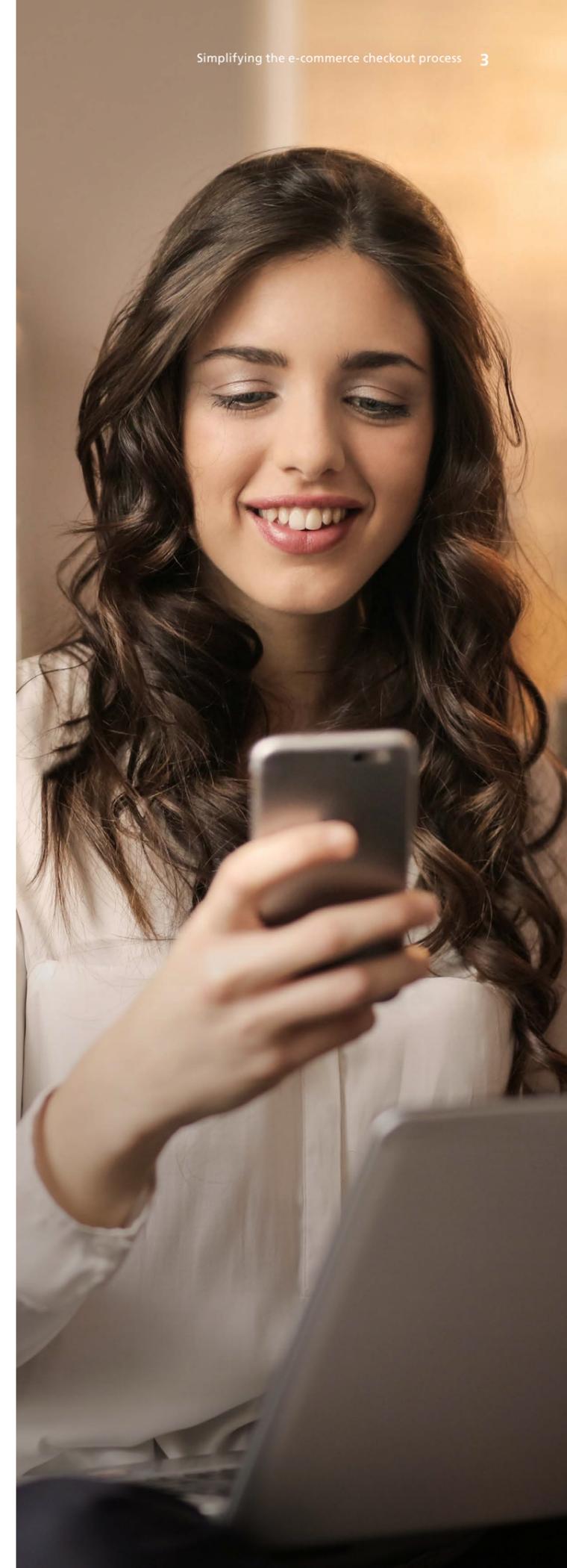
# Future Banking – It is all about Securing Payments!

Did you know? Giesecke+Devrient (G+D) technology is unconsciously used by billions of people every day! With more than 700 global Banks putting their trust in G+D and our offerings, we enable secure and convenient transactions for everyday usage.

Founded in 1852 in Leipzig as a printer of bank notes, now with HQ in Munich, G+D is a global powerhouse in payments - be via cash, card or digital services. Our safe payments technology, elegantly combined with smooth customer experiences throughout the whole customer journey, secures the daily life use of financial services. And also creates customer obsession for our clients!

We are: pioneers in payments, industry leader and innovating partner for the financial sector.

**Giesecke+Devrient**

Giesecke+Devrient Mobile Security GmbH
Prinzregentenstrasse 159
81677 Munich
Germany

www.mobile-security.gi-de.com/futurebanking
mobilesecurity@gi-de.com

Follow us on: