




ULRIKE LINDE

STRATEGIEN
FÜR DIE DIGITALE
GESELLSCHAFT

EIDAS IN THE EUROPEAN FINANCIAL SECTOR: USE CASES AND COMPLIANCE

7. CA-Day, Berlin

Ulrike Linde, Colinde GbR



Financial institutions may act
as a Trust Service Provider
or
as a Relying Party

OPEN BANKING AND OPEN INFRASTRUCTURES

Providing open APIs and interfaces to third parties as FinTechs can be regarded as a challenge or as an opportunity for new business models

- Open APIs should be based on an open infrastructure

The revised Payment Service Directive 2015/2366 (PSD2) sets the legal framework for innovations in the payment infrastructure

- The Account Servicing Payment Service Providers (AS PSP) are obliged to implement open interfaces allowing to initiate payments via Payment Initiation Service Providers (PISP)
- PSD2 does not require that AS PSP must rely on the security infrastructure of third parties, AS PSP remain in control of their own security
- The challenge is therefore to specify state-of-the-art interfaces integrating the customer authentication procedures defined by the ASPSP

THE E-PAYMENT PARADIGM

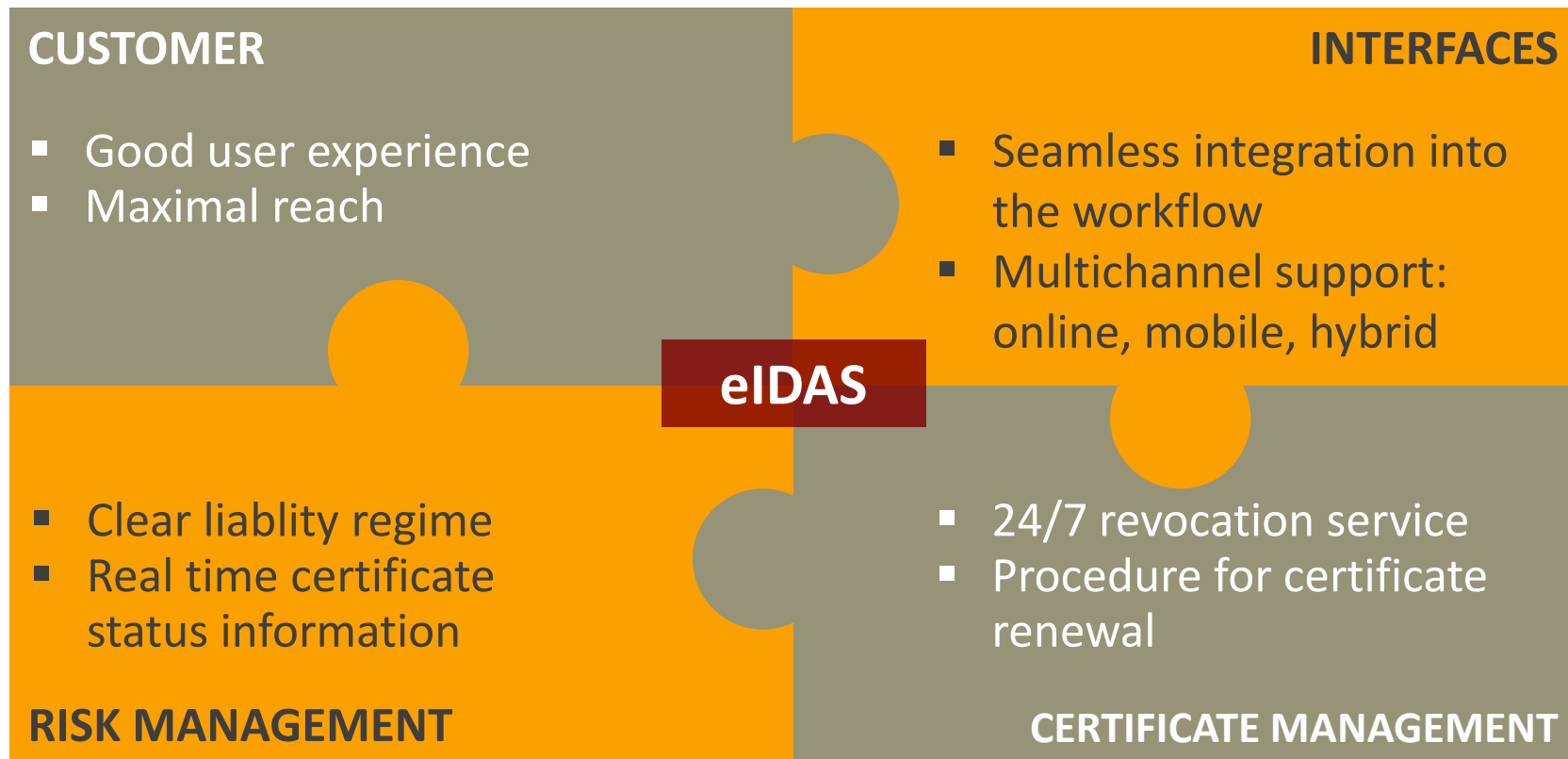
The **customer** does not want to pay, he/she just wants to buy

- Payment is an inherent part of the checkout process
- The customer identifies and authenticates himself only once during the process
- Only for high risk transactions an additional authorisation is acceptable

The **merchant** does not want to invest in technology, he/she just wants to sell

- The first priority is reach > customer basis
- The second one is conversion
- The merchant or his service provider has risk management procedures in place

REQUIREMENTS FOR THE INTEGRATION OF TRUST SERVICES IN FINANCIAL SERVICES



PSD2 REQUIREMENTS ON STRONG CUSTOMER AUTHENTICATION

PSD2 was put in place to boost transparency, innovation and security in the European payments market

- Especially PSD2 establishes a stricter regime of payment service user authentication

The European Banking Authority (EBA) has published a Consultation Paper on the Regulatory Technical Standard* specifying the requirements on

- Strong Customer Authentication (SCA)
- The exemptions from the application of strong customer authentication
- The protection of the confidentiality and the integrity of the payment service users' personalised security credentials
- Common and secure open standards of communication for the transmission of the authentication token

THE USAGE OF PSD2 COMPLIANT SCA FOR SERVER BASED SIGNATURES

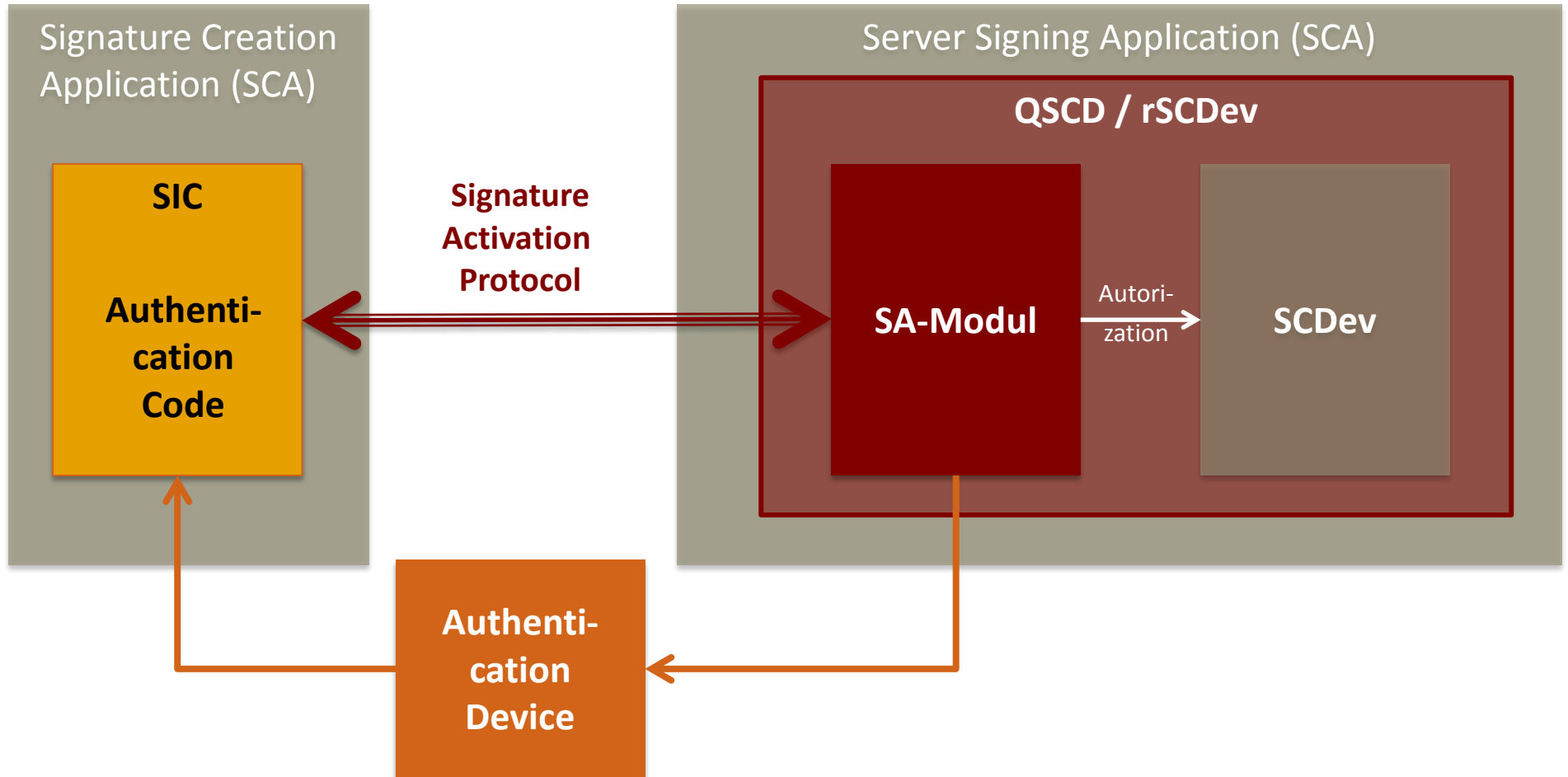
For remote signature scenarios the procedures and mechanisms for strong customer authentication that meet the requirements of the EBA RTS should also be acceptable for the initiation of remote qualified electronic signatures

- The authentication service provided by the AS PSP becomes an eIDAS conformant module of the security infrastructure of the Trust Service Provider

Advantages

- The customer uses the authentication procedure provided by the AS PSP regularly
- Fraud prevention measures are in place
- The cost of the issuance of an authentication token can be translated into a transaction oriented price model

OVERVIEW AUTHENTICATION SERVICE



ANTI-MONEY LAUNDERING REQUIREMENTS

EU directive 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (Anti-money laundering directive) enforces the requirements on customer identification

The KYC principle is laid down in Article 13 (1)

- Customer due diligence measures shall comprise identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source

The implementation of this requirement into national law depends on the (electronic) identification schema in place and the local supervisory regime

THE EIDAS REGULATION DEFINES A COMMON TRUST LEVEL ON IDENTIFICATION

The eIDAS regulation defines for the first time a neutral benchmark for secure electronic identification

- Member States must decide whether they will refer to eIDAS conformant identifications in their national legislation and supervisory practices

The equivalence of the anti-money laundering identification and the identification according to the eIDAS level "high" (or "substantial"?) should be established on European level in order to guarantee a level playing field for all European Trust Service Providers

- The identification service provided by the AS PSP becomes an eIDAS conformant module of the security infrastructure of the Trust Service Provider

OPENING A (CURRENT) ACCOUNT

What are the relevant requirements?



What are the use cases for appropriate eIDAS services?

PRE-CONTRACTUAL INFORMATION

- Financial institutions and Payment Service Providers must provide the consumer with the information needed to compare different offers in order to take an informed decision on whether to conclude an agreement
- Reach and conversion for potential customers must be guaranteed



- (Qualified) electronic seals could assure the integrity and authenticity of this information, especially when there is no secure online banking session
- But there is no such legal requirement

AML-IDENTIFICATION

- The customer and the customer's identity must be verified on the basis of documents, data or information obtained from a reliable and independent source
- This applies not only to all new customers but also at appropriate times to existing customers on a risk-sensitive basis



- A notified identity scheme compliant with the eIDAS regulation should be sufficient for anti-money laundering identification in all European Member States
- When a QES is used for identification purposes the identification data not contained in the certificate have to be send to the financial institution

CONTRACT SIGNING

- Depending on the type of account, in some member states contract agreement must fulfil additional requirements (e.g. accounts with overdraft facility, payment account switching)



- Contract signing may require a qualified electronic signature for specific products according to national legislation
- Signature handling must be integrated in the workflow

ISSUANCE OF AUTHENTICATION MEANS

- The delivery of personalised security credentials, authentication devices and software to the payment services user shall be carried out in a secure manner
- PSD: 24/7 revocation service with clear liability shift
- Authentication procedures shall contain transaction monitoring



- SW used in the authentication procedure must be provided from a trusted source. HW used must contain a trust anchor. A trust scheme between suppliers and issuers of authentication means could be based on eIDAS Services
- When electronic signatures shall be used to authorize payments, real time certification status information with > 99,99xx availability is strictly necessary

ACCOUNT LOGIN

- The application of SCA is exempted where the payer accesses exclusively the information of its payment account online
- SCA shall not be exempted where the payer accesses his account for the first time or later than one month after SCA was applied



- For SCA see transaction authorization

TRANSACTION AUTHORIZATION – STRONG CUSTOMER AUTHENTICATION

SCA with dynamic linking has to be used in the following use cases

- Initiation of credit transfers initiated via the online/mobile banking of the payer
- Authorization of card transactions
- Authorization of direct debit e-mandates
(not the initiation of a direct debit based on an agreed mandate)



- Electronic signatures can only be used for the initiation of credit transfers and card transactions if the payer's PSP supports these as authentication procedure
- In the case of direct debits, the payee may decide to accept e-mandates signed electronically by the payer

TRANSACTION AUTHORIZATION – PAYMENT INITIATION

- The communication interface provided by the AS PSP shall allow PISP to rely on the authentication procedures of the account servicing payment service provider
- In this interface AS PSP shall identify the PISP who wants to access the account of the customer by using the authentication procedure provided by the AS PSP



- For the purpose of identification, payment service providers shall rely on Qualified certificates for website authentication as per article 3(39) of the eIDAS regulation
- The registration number of the certificate shall be the authorization number granted by the financial supervisory authority of the home member state

ACCOUNT BILLING STATEMENT

- Electronic account billing statements are electronic invoices, when the tax to be applied is a VAT
- The requirements on integrity and authenticity relevant for electronic invoices have to be fulfilled



- Applying internal controls to account billing statements is much more difficult for bank customers as there are no additional documents as orders, delivery notes etc.
- If the bank customer does not want to recalculate the service fees and taxes each time, the protection of account billing statements with (qualified) electronic seals could provide an appropriate protection

CONCLUSION

The integration of the eIDAS infrastructure is not imposed in the regulatory framework for financial services

Trust services must be attractive and flexible, leveraging the three dimensions

- User experience
- Security/liability
- Business model

Financial institutions must change their mind-set and business models in order to rely on open trust infrastructures

- Clarify the roles as issuer of authentication procedures and relying party
- Using PKI technologies for authentication procedures enables the definition of state-of-art interfaces to third parties as PISP and FinTechs

ULRIKE LINDE

STRATEGIEN FÜR DIE DIGITALE GESELLSCHAFT

Altenberger Weg 11

13156 Berlin

Deutschland

T +49 (0)30 47 475 744

M +49 (0)179 21 22 548

ulrike.linde@colinde.de

