Finnish Instant Payments Scheme Rulebook

The work on the concept covering the Scheme and the Governance model was mandated by the Finnish Payments Council and was created as a market-based initiative. The work was coordinated by the Bank of Finland in its role as the chair of the Finnish Payments Council. The Finnish Instant Payments Scheme Rulebook (the Scheme, the Rulebook) will be owned by a non-profit Association (the Association) established under and governed by Finnish law. Membership of the Scheme is open to all parties who agree to adhere to the principles of the Rulebook.

The design of a solution enabling instant payments has been scoped, in its initial phase, to two use cases: consumer payments at points of sale (POS) and person-to-person (P2P) payments. With regard to the consumer applications, the Finnish instant payment solution will be implemented as a mobile application adhering to the Rulebook and following the implementation guidelines with the exact functionality and appearance of the application being determined on the discretion of each individual service provider.

The solution must follow pan-European instant payment practices, such as the SEPA Instant Credit Transfer Scheme Rulebook and SEPA Request-to-Pay Scheme Rulebook, and requirements as described in the implementation guidelines. Settlement must be done in a central bank system.

A smooth and convenient user experience is a key component for the success of the Scheme. While the consumer applications can be developed by all adhering service providers, a set of mandatory and optional user requirements described. The requirements cover expectations for payer and payee, merchant, and service provider. Mandatory features cover characteristics like frictionless transactions, user friendly payer authentication, and simplicity for enrollment, trust and security, cost-effectiveness, and customer focus. Optional features cover characteristics like loyalty programs or rewards and other value-added services associated with the payment transaction as a single show payment.

The payment service user (PSU) can either be the consumer initiating the payment (the Payer), or the consumer or merchant receiving the payment (the Payee) e.g. for selling goods or services to the Payer. The PSU does not have a direct contract or relationship with the Scheme. Consumer agreements are separately drafted between PSUs and their Payment Service Providers (PSPs). To do a payment, the PSU must have an account with an Account Servicing Payment Service Providers (ASPSP) that is part of the Scheme. A Merchant User (MU) has a direct contract with a PSP to accept payments. MU is the initiator for the request-to-pay (RTP) process and is the ultimate beneficiary of the inbound transaction. MU must be a customer of a SEPA Instant Credit Transfer reachable ASPSP.

Payer’s PSP provides payment service to the consumer. Payer’s PSPs must offer both a P2P payment method and a payment method for POS payments. Payee's PSPs offer services to Payment Service Users that can be either Merchant Users or Consumers or both. Acceptance at the point-of-sale (POS) must be possible with QR-code technology. Other possible technologies (e.g. NFC) can be agreed in the Scheme. Payer's and Payee's PSPs are part of the RTP network. Payee's PSP creates the RTP message that is sent to the RTP network.

ASPSP can offer access to the consumer account by a third-party application, or it can offer the payment service itself. Strong Customer Authentication (SCA) delegation is mandatory from ASPSP towards PSP. Pricing of risk needs to be determined based on objective risk exposure of the PSP. Each service provider chooses its own SEPA Request-to-Pay (SRTP) network provider, provided that the SRTP networks are interoperable.

Payment institutions adhering to the Scheme need to comply with the Directive (EU) 2015/2366 (Revised Payment Services Directive, PSD2) in the authentication process. The payment service providers should provide the possibility for SCA exemptions, as per Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366, where applicable. The user needs to authenticate itself in the following cases: 1) onboarding, 2) opening payment application, 3) payment initiation, 4) payment authorisation, and 5) offboarding.

Registration can be done from any Scheme and Rulebook compliant application. The user can register multiple accounts with several ASPSPs, but one needs to be chosen as the default account for receiving payments. A verified mobile phone number will be used as alias for receiving instant payments and payment requests. To offboard, the user can use any active rulebook compliant application the user has used to on-board.

For Person-to-person (P2P) instant payments a central Proxy Registry / Proxy Lookup Service is provided by a designated Proxy Registry Service Provider to all the Participant PSPs. The central Proxy Registry provides the necessary proxy services for all the Participant PSPs by mapping End Customer Proxy information (mobile phone number as default) to End Customer PSP and End Customer account number (IBAN). P2P instant payment can be initiated with or without Request-to-pay.

Processing a POS transaction contains two phases. In the pre-processing phase the end-user (Consumer) is enabled with the ability to use the product, i.e. originating a payment mandate (PM). The PM is single use, single transaction, and tied to the payer's payment account. The payer's ASPSP creates the PM based on a request from the Payer's PSP. It includes a mandate to start a single transaction and other control information needed during the payment process e.g. information related to the loyalty programs or electronic receipts. A batch of payment mandates can be created in advance to be stored within a payment solution provided by the payer's PSP. The PSP and the ASPSP are in a bilateral agreement on the delegation of SCA processes from the ASPSP to the PSP processing the transactions on ASPSP's behalf. SCA delegation includes the formal agreement on risk-transfer policies between the entities.

In the payment processing phase, the Payer displays the PM to the Payee. Payee creates the SEPA RTP request and after validation it is displayed to the Payer who has to actively approve the request. Following the approval, the Payer's PSP initiates the SEPA Instant Credit Transfer instruction.

The Scheme participants shall ensure security and manage together the risks of running the Scheme. For this they shall put in place a risk management framework that defines the roles and responsibilities and the overall risk management activities of the Scheme, and a set of procedures and processes to identify potential adverse events and for minimising their impact.