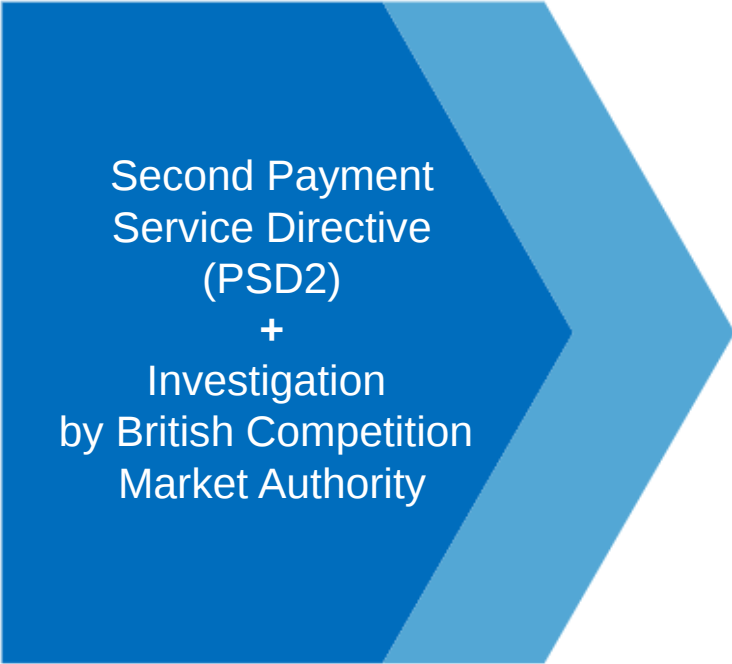


Design and Implementation of a Data-Driven, Provider-Independent Test Service for Banking APIs

Josef Kamysek, 27. January 2020, Garching Forschungszentrum

Chair of Software Engineering for Business Information Systems (sebis)
Faculty of Informatics
Technische Universität München
www.matthes.in.tum.de

- Motivation
- Challenges and issues
- Main actors of access to account (XS2A)
- Model of test tool
- Overall goal and research questions
- Initial results
 - Main steps to access a PSD2-compliant interface from a high-level perspective
 - Encountered problems and potential solutions
- Next steps
- Timeline



Second Payment
Service Directive
(PSD2)
+
Investigation
by British Competition
Market Authority

- Third Party Providers get right to access user accounts
- Strong customer authentication
- Improved consumer data protection
- Foster competition and innovation
- Interface for Third Party Provider

Efficient test process is necessary!

- Increase quality and stability
- Reduce test effort
- Reduce testing costs
- Improve error handling

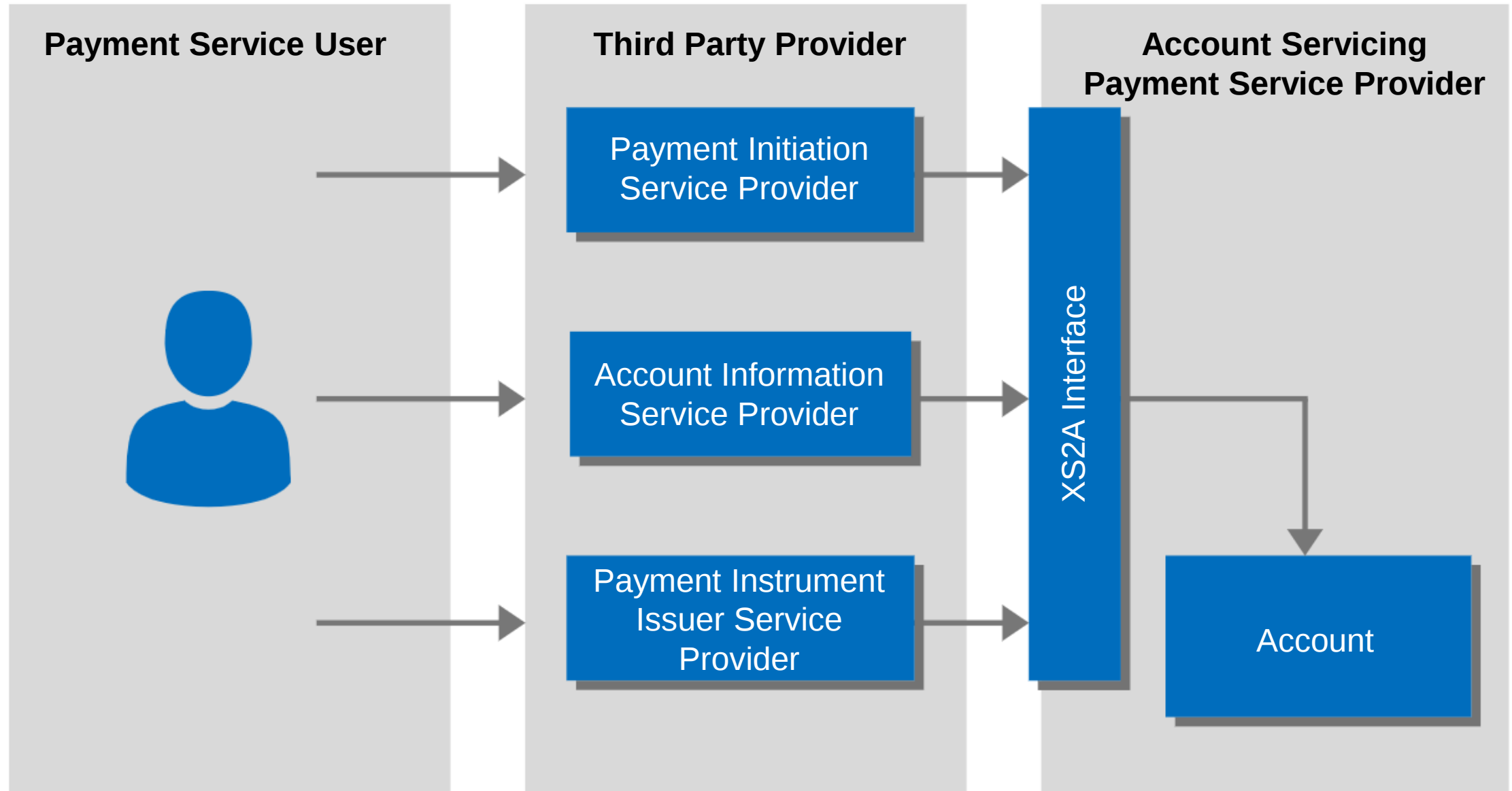
Challenges and issues

- Deadlines, time pressure and high expenditure
 - Shortening or omission of test procedures
- Software errors
 - Damage company reputation and change product attitude of customer
- Banks responsible for their testing process
 - Differences in test environment and test coverage
- Test process of PSD2-compliant APIs is time consuming, complicated and error-prone

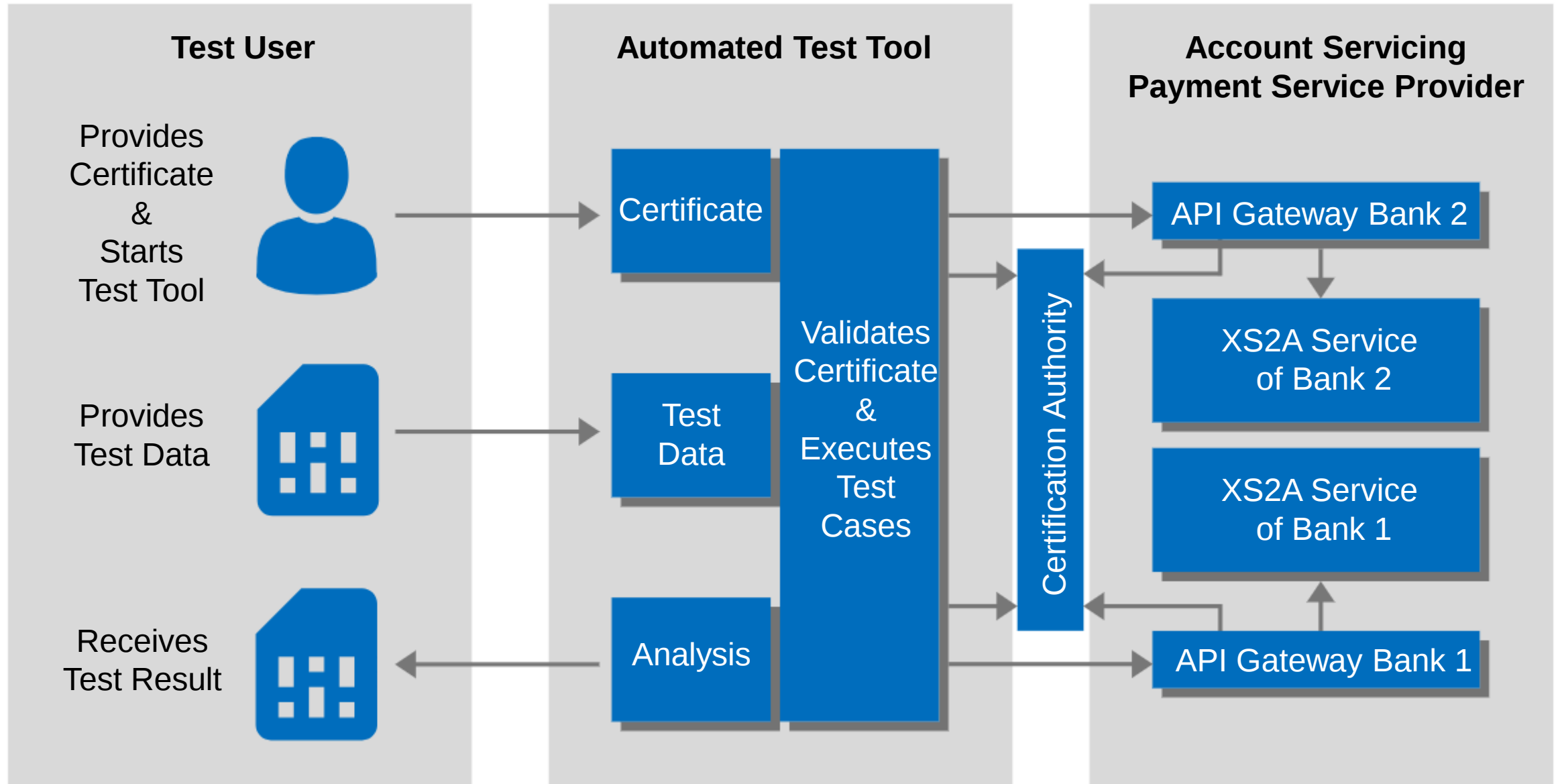


How can an efficient test process be performed using a data-driven and vendor-independent test tool?

Main actors of access to account (XS2A)

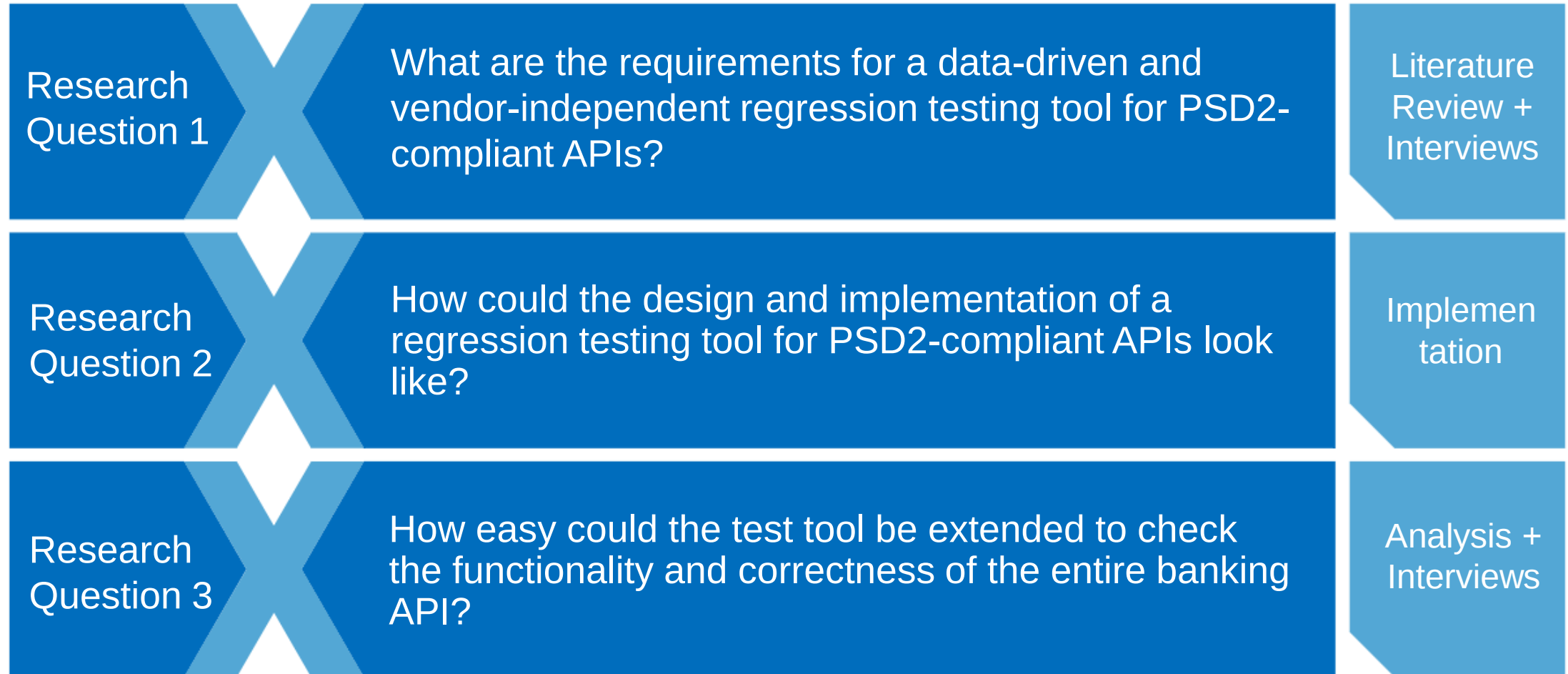


Model of test tool



Overall goal and research questions

Goal: Establishment of an efficient test process of PSD2-compliant APIs by using regression tests in a data-driven and provider independent test tool



Main steps to access a PSD2-compliant interface from a high-level perspective

Only done once

Registration

Onboarding

Authentication

Workflow

Repeated for each request

Encountered problems and potential solutions (1)



- Registration with national authority (e.g. in Germany → BaFin)
- Elaborate application procedure, which can take up to half a year
- Third Party Provider must disclose their business model

→ If the national authority considers Third Party Provider to be trustworthy, an eIDAS-compliant certificate can be obtained

Problem:

- Only companies can register with the national authority, individuals cannot
- No certificate can be obtained without recognition by the national authority

Encountered problems and potential solutions (2)



- Banks need Qualified Web Authentication Certificate (QWAC) for onboarding process of Third Party Provider
- Qualified certificates have to be issued by Qualified Trust Service Provider (QTSP)
- Certificate is for electronic identification and trust services for electronic transactions

Problem:

- Certificates are only issued to companies that are registered with a national authority
- Bank interfaces are not accessible without a certificate

Current solution:

- Use of a local sandbox

Encountered problems and potential solutions (3)

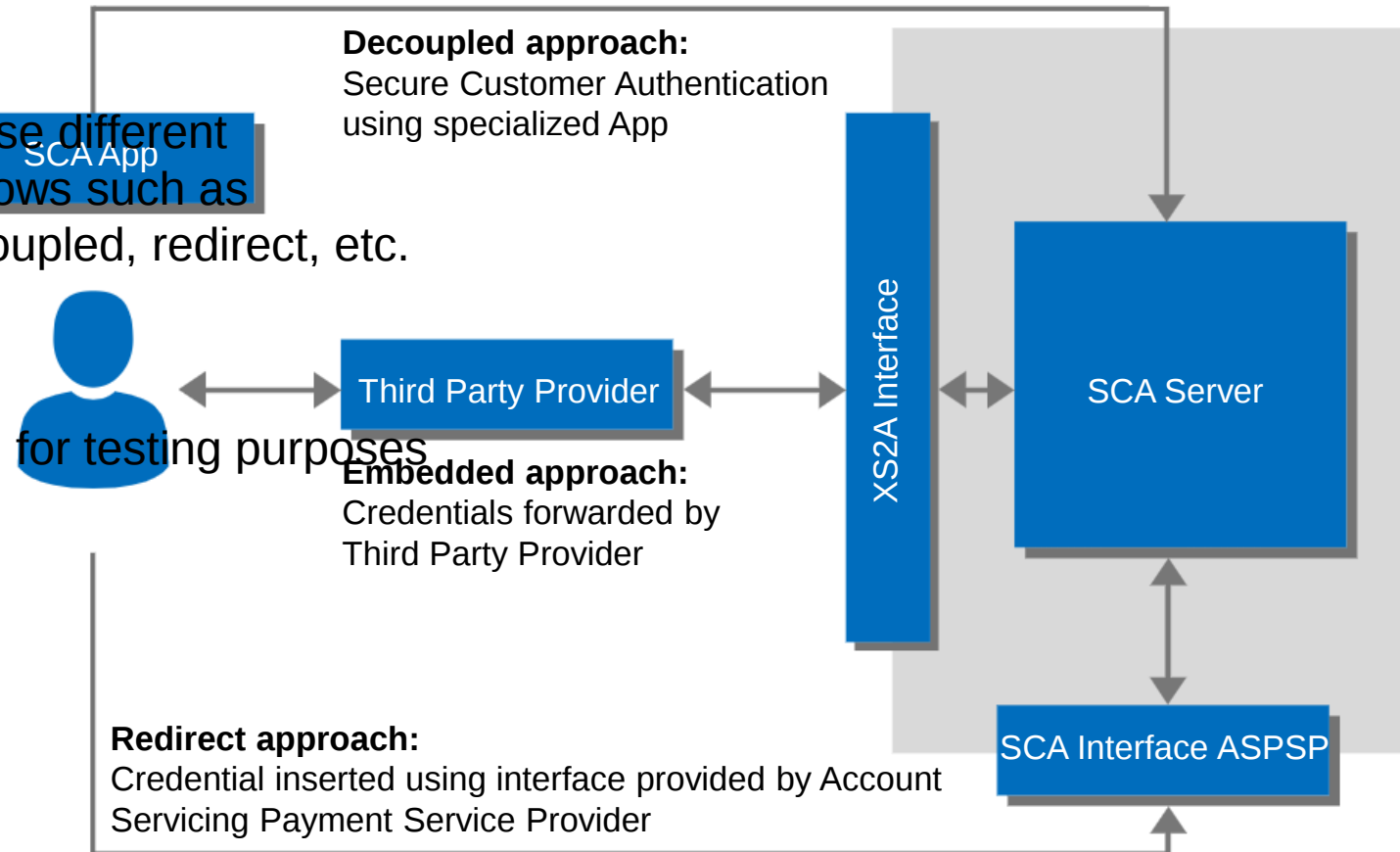


Problem:

- Banks can choose different authentication flows such as embedded, decoupled, redirect, etc.

Current solution:

- Store static TAN for testing purposes



Encountered problems and potential solutions (4)



- API workflows are defined in specifications and operational rules
- Example: access account information
 - Establish account information consent
 - Get list of reachable accounts

Problem:

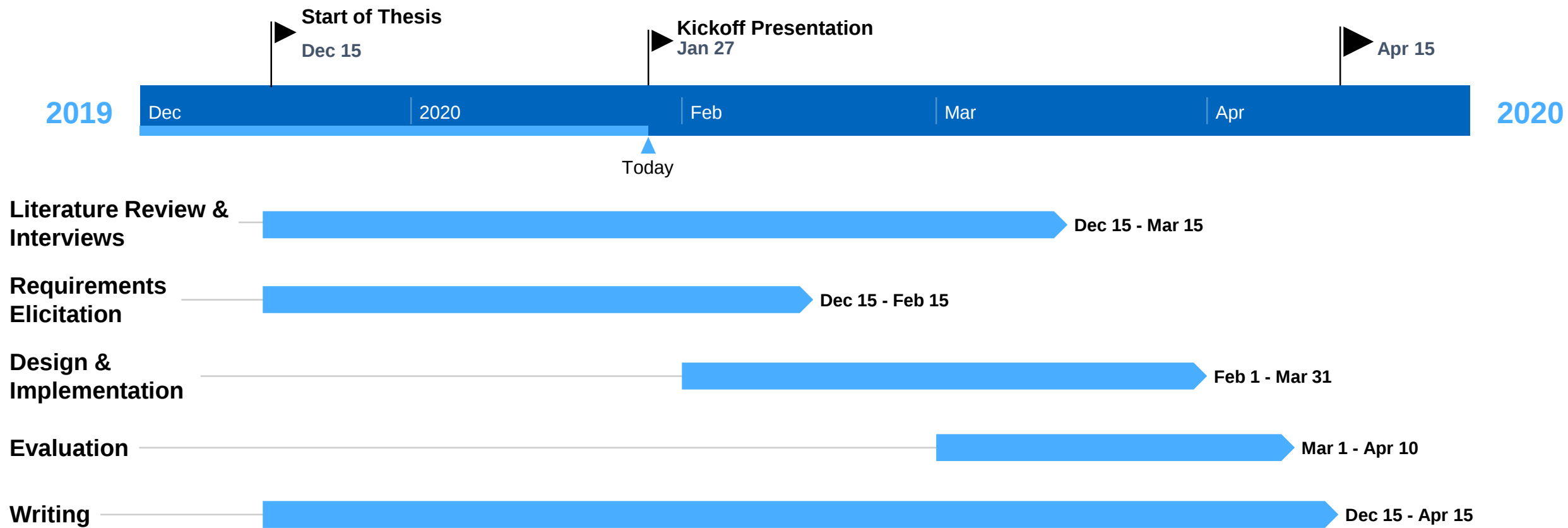
- In theory each bank can develop own proprietary XS2A communication standard
- No EU wide standard leads to high diversity of interfaces
- Banks make minor changes to interfaces → flavors

Current solution:

- Focus on most common “standard” → Berlin Group

Next Steps

- Further expert interviews
- Additional literature research
- Creation of test specification and test plan
- Implementation of test tool



- [1]: A. Smith, T. Hoehn, P. Marsden, J. May, and E. Smith, "Retail banking market investigation - final report," 2016. <https://assets.publishing.service.gov.uk/media/57ac9667e5274a0f6c00007a/retail-banking-market-investigation-full-final-report.pdf>.
- [2] E. Parliament, "Directive (eu) 2015/ of the european parliament and of the council of 25 november 2015 on payment services in the internal market, amending directives 2002/65/ec, 2009/110/ec and 2013/36/eu and regulation (eu) no 1093/2010, and repealing directive 2007/64/ec." <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=EN>.
- [3] T. Lynn, J. G. Mooney, P. Rosati, and M. Cummins, eds., Disrupting finance: FinTech and strategy in the 21st century. Palgrave Pivot, Cham: Palgrave Macmillan, 2019. <http://hdl.handle.net/10419/191566>.
- [4] Edgescan, "Payment services directive (psd2) - opening the doors to a secure business." <https://www.edgescan.com/wp-content/uploads/2018/05/psd2.pdf>.
- [5] KPMG in the UK, "Psd2 testing considerations." <https://home.kpmg/content/dam/kpmg/uk/pdf/2019/07/psd2-testing-considerations.pdf>.
- [6] H. Mohanty, J. R. Mohanty, and A. Balakrishnan, eds., Trends in Software Testing. Singapore and s.l.: Springer Singapore, 2017. <http://gbv.ebib.com/patron/FullRecord.aspx?p=4613345>.
- [7] C. D. Nguyen, "Testing techniques for software agents." https://pdfs.semanticscholar.org/d558/743ba0a12c29144a3e4a24c36f81dea0a21a.pdf?_ga=2.45937316.1634729274.1578388548-1301065639.1578388548.
- [8] P. A. Jeff Offutt, "Why do we test software?," 12.11.2018. <https://cs.gmu.edu/~offutt/softwaretest/powerpoint/Ch01-whyTest.pptx>.
- [9] Alan R. Hevner, Salvatore T. March, Jinsoo Park, and Sudha Ram, "Design science in information systems research." https://wise.vub.ac.be/sites/default/files/thesis_info/design_science.pdf.
- [10] PSD2 Regulation, Strategy, Innovation <https://www.finextra.com/blogposting/18057/psd2-regulation-strategy-and-innovation>
- [11] PSD2 - Second Payment Services Directive, Information Set, <https://www.financelatvia.eu/wp-content/uploads/2018/04/PSD2-Second-Payment-Services-Directive-.pdf>
- [12] Interview Partner 1
- [13] Interview Partner 2

Backup

Establish consent

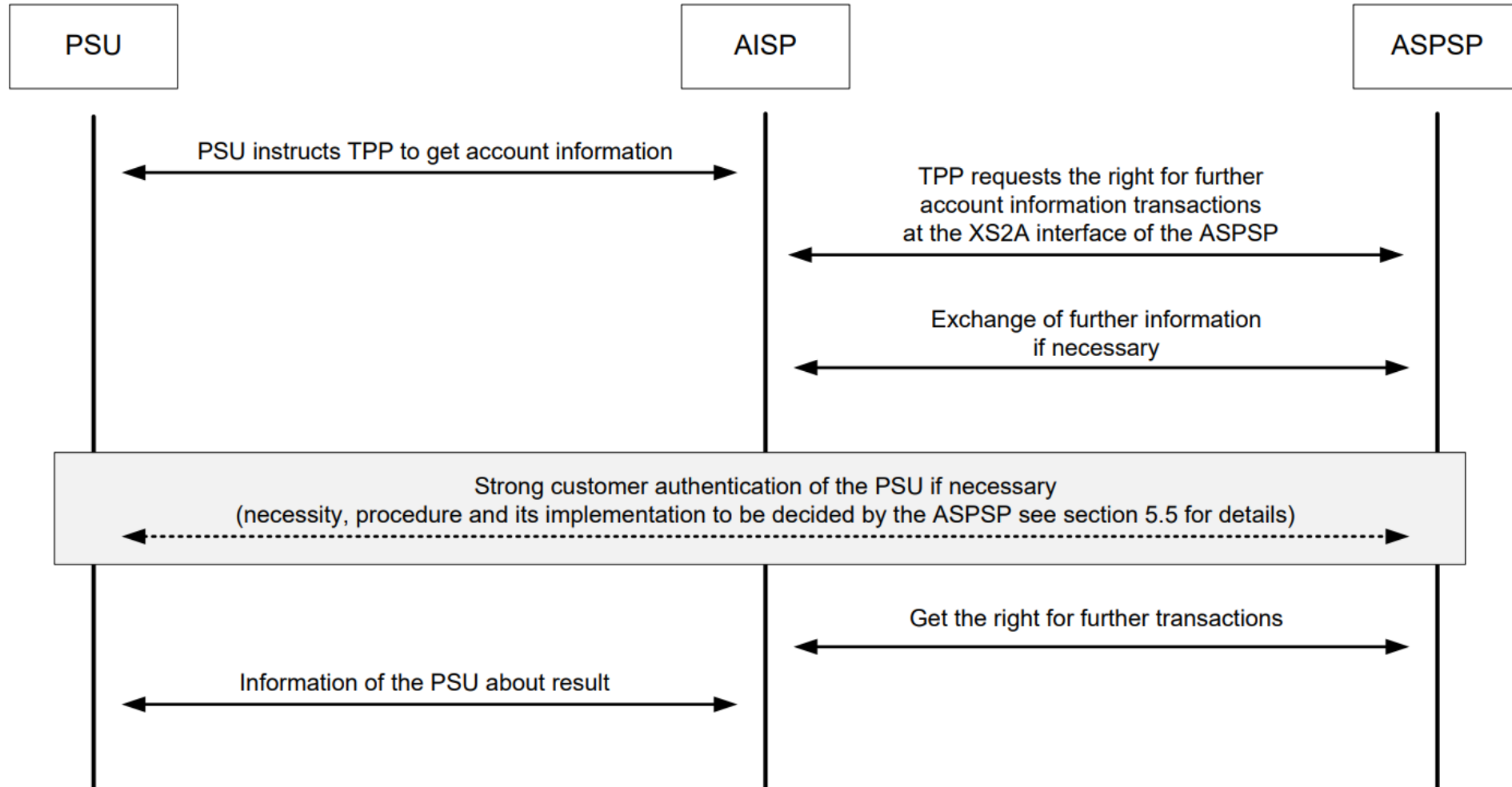


Figure 8: Use case Establish account information consent

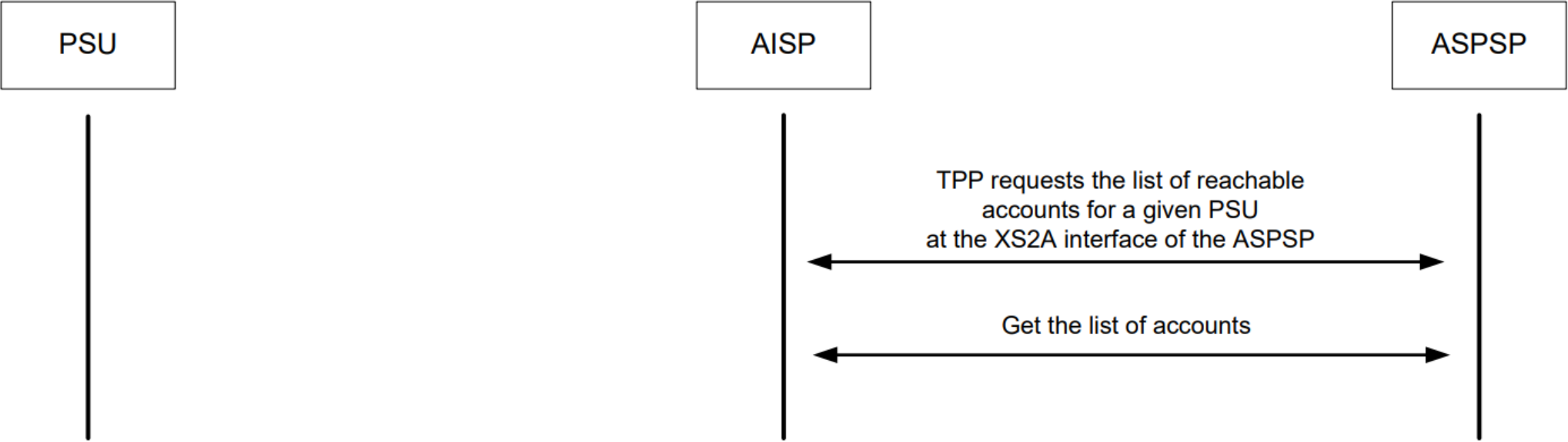
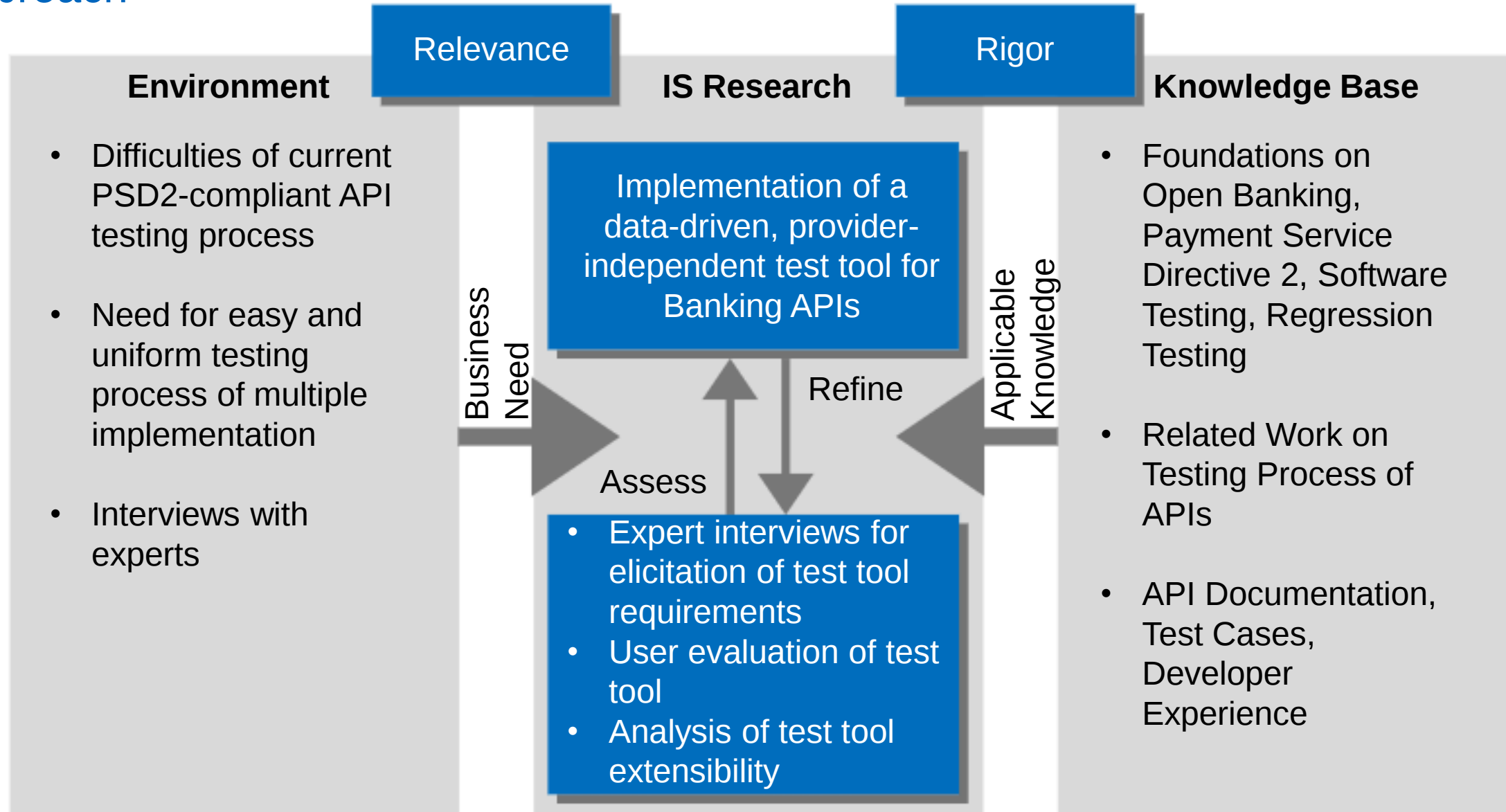


Figure 9: Use case Get list of reachable accounts



Why is a new test tool needed?

Flexibility and freedom

Reusability of code

Few limitations while designing data-driven automation framework

Domain specific language allows behavior-driven tests

API Calls Swagger

GET	/v1/accounts	Read account list	🔒
GET	/v1/accounts/{account-id}	Read account details	🔒
GET	/v1/accounts/{account-id}/balances	Read balance	🔒
GET	/v1/accounts/{account-id}/transactions	Read transaction list of an account	🔒
GET	/v1/accounts/{account-id}/transactions/{transactionId}	Read transaction details	🔒
POST	/v1/consents	Create consent	🔒
GET	/v1/consents/{consentId}	Get consent request	🔒
DELETE	/v1/consents/{consentId}	Delete consent	🔒
POST	/v1/consents/{consentId}/authorisations	Start the authorisation process for a consent	🔒
GET	/v1/consents/{consentId}/authorisations	Get consent authorisation sub-resources request	🔒
GET	/v1/consents/{consentId}/authorisations/{authorisationId}	Read the SCA status of the consent authorisation	🔒
PUT	/v1/consents/{consentId}/authorisations/{authorisationId}	Update PSU data for consents	🔒
GET	/v1/consents/{consentId}/status	Consent status request	🔒