SFTI - working group 'Common API'

Cyber Security - API Thread Modelling

White Paper

Authorship: Swiss FinTech Innovations
Release: Version 1.0
Date: 29.03.2023

Authors

Leo Bolshanin (Adnovum), Patrik Schmid (Adnovum) - Reviewed by SFTI's Common API working group community

About SFTI

Swiss Fintech Innovations (SFTI) is an independent association of Swiss financial institutions committed to drive collaboration and digital innovations in the financial services industry. For more information about *Swiss FinTech Innovations*, please refer to http://www.sfti.ch.

Content

1. Introduction

1.1 Objective

The objective of an Information Security and Data Privacy (ISDP) concept is to identify threats pertaining to a given Information System, to propose security measures likely to mitigate risks associated to those threats and evaluate the residual risks.

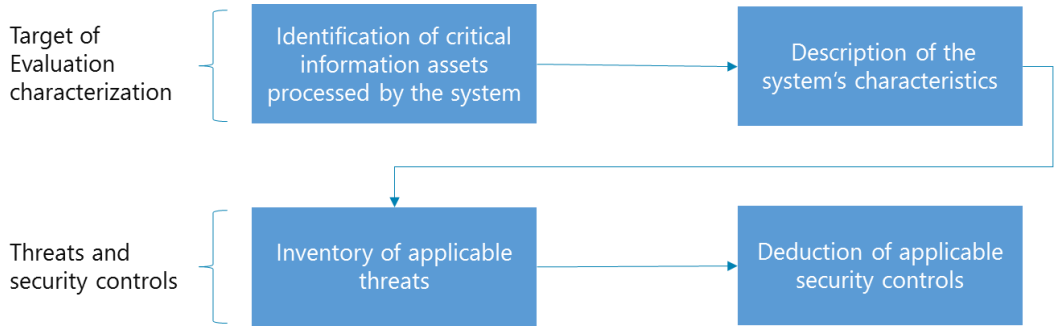
1.2 Scope

The system examined in the present ISDP concept are the open API's as specified in the SFTI Common API. These APIs cover functionality for customer management (contracts, persons, addresses, KYC, …), custody services (accounts, portfolio, …), security trading, payments, credit cards, mortgages etc.

The scope of the document was intentionally left broad to provide general guidance for the definition, evolution and application of open API's. Specific risks following the individual business use cases of API's will need to be looked at separately and in conjunction with the respective API. The thread scenarios and mitigations are though generically applicable.

1.3 Methodology

The diagram below shows the successive steps of the methodology applied to realize the present ISDP concept.



1.4 Exclusions

We intentionally chosen the context of APIs as driven out of the perspective of a financial institution. This choice was made to exclude risks related to the maintenance of the hardware, operating system, software, organization or physical disasters already managed within the risk framework of a financial institution.

1.5 References

Ref	Document
Wealth-API [1]– ein neuer Schweizer Standard	https://swissfintechinnovations.ch/wp-content/uploads/2017/12/Multibanking-WhitePaper_bySFTI.pdf
Specification of Wealth API for Security Trading	https://common-api.ch/index.php/en/resources-en/swagger-files?id=70
Specification of Wealth API for Custody Services	https://common-api.ch/index.php/en/resources-en/swagger-files?id=71
Specification of Wealth API for Customer Management	https://common-api.ch/index.php/en/resources-en/swagger-files?id=72
OWASP API Security Project	https://owasp.org/www-project-api-security/

[1] The Wealth API was leverage as a reference point for the discussion and to validate thread scenarios and mitigating actions.

2. Target of evaluation characterization

2.1 General description

Threat modelling exercise for the Common API's (X2A, Payment, Mortgages etc.) as discussed and defined in the SFTI workgroup.

2.2 Information assets processed

This chapter lists the various types of data processed, their requirements in terms of confidentiality (C), integrity (I), availability (A) and compliance, and the impact areas in case of compromise.

2.2.1 Assets to protect

Name	Owner	C	I	A	Impact Areas
IT Security data	CIO	High	High	Medium	Finance; Legal/Compliance; Reputation
Customer Identifying data	Head of customer relationship	High	High	High	Finance; Legal/Compliance; Productivity; Reputation
Customer Financial Data	Head of customer relationship	High	High	High	Health/Life; Finance; Legal/Compliance
Indirect Customer Identifying Data	Head of customer relationship	High	High	High	Health/Life; Finance; Legal/Compliance
Customer credentials	End Customer	High	High	High	Health/Life; Finance; Legal/Compliance; Productivity; Reputation

2.3 Other characteristics

The table below summarizes some of the ToE's characteristics which allow to identify the applicable threats to it.

Hosting mode	IaaS
Internal software development involved	Yes
External software development involved	No
Data extract	No (extracting real data from the production environment for test purposes)
Use Third Party Service	Yes (potentially using third party services, external to the financial organization, by one of the API functions)

2.4 Threat agents

The table below is a typology of threat agents that may affect the security of information systems related to open APIs.

Origin	Possible threat agents	Possible motivations	Possible outcomes
Internal	Employee, contractor	Challenge, fame, monetary gain, political gain, intelligence, nuisance, negligence	Information disclosure, information modification, interruption of service, Information destruction/loss, illicit transfer of assets
External	Internet hacker, competitor, supplier, ex-employee, state agency, terrorist group		

The table below lists the agents, which represent a potential threat to the ToE.

Label	Threat Agent Type
Third Party Provider (TPP - incl. fintechs)	Human external with technical means - Other
Internet-based threat actor	Human external with technical means - Other
Employee with technical access	Human internal with technical means
IaaS provider employee with physical access	Human external with physical access - Supplier
IaaS provider employee with technical access	Human external with technical means - Supplier
Legitimate user with compromised device	Human external with technical means - Other
Open Banking service layer provider with technical access (disgruntled employee)	Human external with technical means - Other
Trusted Central Authority (disgruntled employee)	Human external with technical means - Other

2.5 Technical and other problems

The table below lists technical and other problems likely to affect the security of information systems related to open APIs.

API implementations must account for these and ensure consistency in the transaction handling and processing.

Possible problem	Examples
Environmental hazard	e.g. lightning, flooding, fire
Hardware defect	e.g. component failure, bottleneck
Software defect	e.g. application crash, application bug
Supporting utility failure	e.g. network, telecommunications, air conditioning
Compliance issue	e.g. Intellectual property violation, data protection law compliance issue
Hosting/Cloud computing risks	e.g. Access to data by foreign authorities, lack of data isolation/separation, lack of integration with IAM, lock-in-effect, loss of control on data protection, service unavailability

3. Threat Scenarios

The following table lists the threats that apply to the Target of Evaluation's context:

Documentation

Category	Name	Prerequisites	C	I	A	Likely threat agent(s)	Mitigations
Conceptual documentation	Lack of consistent documentation Lack of architecture and security concept documentation Failure to maintain the documentation up to date	N/A	M	M	M	• N/A	• Application architecture • Security concept (set of mitigations, based on risk assessment) • Deployment diagram • API documentation (ex. Swagger, usage documentation, simple code) • Source code documentation • Documentation change management process
Documentation of operations	Lack of description of operational processes	N/A	M	M	M	• N/A	• Documentation of operational processes • Change management in operations

TPP management

Category	Name	Prerequisites	C	I	A	Likely threat agent(s)	Mitigations
TPP registration	Registered client application could be malicious	TPP registration	H	M	M	• Third Party Provider (TPP - incl. fintechs) • Trusted Central Authority (disgruntled employee) • Open Banking service layer provider with technical access (disgruntled employee)	• Security assessment to validate the TPP and contractual obligations • Admission criteria for TPP registration
TPP governance	Orphan TPPs, TPPs could become malicious during their life cycle	TPP registration	H	M	M	• Third Party Provider (TPP - incl. fintechs)	• Detect orphan TPPs on data of usage monitoring • Revalidate client applications and update the contractual obligations on a regular basis
TPP governance	Social engineering	Contact with human agent linked to the target system	H	M	M	• Third Party Provider (TPP - incl. fintechs) • Internet-based threat actor • Trusted Central Authority (disgruntled employee) • Open Banking service layer provider with technical access (disgruntled employee)	• Security awareness program for employees • Transparency on certified TPP's and changes • Firm customer and partner identification/authentication process

AAA Authentication, Authorization, Accounting

Category	Name	Prerequisites	C	I	A	Likely threat agent(s)	Mitigations
User authentication	Account hijacking Ex. • Credentials compromise • API2:2019 Broken user authentication	Registered legitimate user account	H	M	L	• Internet-based threat actor • Employee with technical access • IaaS provider employee with technical access • Legitimate user with compromised device	• Out-of-band authentication • Multi-factor authentication • Token/cookie should be stored securely, and token life cycle implemented properly (ex. id, refresh and bearer tokens) • Session management implemented • Enforce minimal standards and implement controls / audits
User authentication	Orphaned User	Registered legitimate user account	H	M	L	• Internet-based threat actor	• Monitoring of end user activity • Deactivation of orphaned users
Client application authentication	Malicious client application pretends to be a registered TPP	Registered legitimate TPP	H	M	M	• Third Party Provider (TPP - incl. fintechs) • Internet-based threat actor	• Require client ID and client secret for granting access • Urge TPP to treat credentials securely
API authorization	Unauthorized access to data	API accessible to attackers	H	M	L	• Third Party Provider (TPP - incl. fintechs) • Internet-based threat actor • Employee with technical access • IaaS provider employee with technical access • Legitimate user with compromised device	• Proper use of delegation protocol (OAuth2) for authorizing API access by TPPs • Creation of API categories and hosting infrastructure domains by API sensitivity
API accounting	Missing traceability on incident investigations	N/A	L	M	L	• N/A	• Log which client uses which API on behalf of whom at what time • Leverage data analytics to identify malicious behaviour (anomalies)

Consent Management

Category	Name	Prerequisites	C	I	A	Likely threat agent(s)	Mitigations
User consent	Organization view: Absence of fine-grained consent User view: Giving extensive consent	Registered legitimate user account	M	L	L	N/A	• Need-to-know principle, explicit fine-grained user consent
User consent governance	Organization view: Outdated consent	Registered legitimate user account	M	L	L	N/A	• Organization must provide transparency adapted to user knowledge

Category	Name	Prerequisites	C	I	A	Likely threat agent(s)	Mitigations
	User view: Outdated consent leads to lack of transparency						• Consent management portal, awareness program, consent expiry, active life cycle management of consent • Actively withdraw consent for unused services, giving minimal consent (privilege minimization)
User consent governance	Access to data outside Switzerland	Registered legitimate user account	M	L	L	N/A	• User needs to provide explicit consent to accessing data outside of Switzerland • Authorization model has to take into account the user consent and user access context (ex. Location, device, etc.) • Authorization policies must cover compliance requirements
User consent governance	Data Protection compliance breach -> Breach with legal or contractual requirements Including consent management issues, such as lack of fine-grained consent, outdated consent	Registered legitimate user account	M	L	L	N/A	• Dataflows need to be documented and privacy assessment need to be conducted • Consent management must be implemented • Define clearly distinguished data room authorizations for each consent • Consents must replicate the underlying authorization and access structures. • Do not allow grandfathering of consents between API versions if other or more data, as consent was granted for, will be delivered. • Perform regular reviews of consents given/received and compare with expectations / agreements

Data Security

Category	Name	Prerequisites	C	I	A	Likely threat agent(s)	Mitigations
Content inspection	Malicious code or data injection Ex. • API1:2019 Broken object level authorization (ex. Lack of user input validation/content type validation) • API5:2019: Broken Function-Level Authorization	API accessible to an attacker Registered legitimate user account used by attacker	H	H	H	• Third Party Provider (TPP - incl. fintechs) • Internet-based threat actor • Legitimate user with compromised device	• Input validation on multiple layers (API implementation, API gateway, WAF) on the level of financial institution

Category	Name	Prerequisites	C	I	A	Likely threat agent(s)	Mitigations
	• API6:2019: Mass Assignment						
Data governance	TPP gets more information than the user wants to give Inadequate data filtering Ex. API3:2019: Excessive Data Exposure	Registered legitimate user account	M	L	L	• Third Party Provider (TPP - incl. fintechs) • Legitimate user with compromised device	• Dynamic fine-grained authorization on data level according to given consent • Data filtering on the backend – only minimal dataset to be sent to TPP • Transparency on data exchanged
Data protection	Storage/processing of data outside Switzerland	Registered legitimate user account	M	L	L	• N/A	• End user "waives" the data for utilization by TPP; TPP, FI and other involved parties must follow the respective data protection rules
Data protection	Information leakage, integrity violation Interception/alteration of data during transport	Attacker access to the information flow between TPP and user or TPP and bank APIs	H	M	L	• Internet-based threat actor • Employee with technical access • IaaS provider employee with technical access • Open Banking service layer provider with technical access (disgruntled employee)	• Encryption of data in transit using TLS or even TLS with additional content encryption/signing
Quota management	Exfiltrating large amount of data	Successful compromise of APIs or TPP functionalities by an attacker	M	L	L	• Third Party Provider (TPP - incl. fintechs) • Internet-based threat actor • Legitimate user with compromised device	• Limit the use of APIs per client (throttling)

API Management

Category	Name	Prerequisites	C	I	A	Likely threat agent(s)	Mitigations
API governance	Unneeded exposed APIs or API versions (shadow APIs)	Exposed APIs	H	M	M	• Third Party Provider (TPP - incl. fintechs) • Internet-based threat actor • Employee with technical access • IaaS provider employee with technical access • Legitimate user with compromised device • Open Banking service layer provider with technical access (disgruntled employee)	• Usage monitoring, integration into security information and event management (SIEM) systems; clear audit trails on API usage; up-to-date inventory of APIs and TPPs • API life cycle and version management • Up to date API inventory – manual or automatic • Testing environments, separated from production • API versioning • Regular audits • Clear change management process

Category	Name	Prerequisites	C	I	A	Likely threat agent(s)	Mitigations
API monitoring and analytics	Undetected brute force attacks or improper use of APIs by legitimate TPPs	Exposed APIs	M	M	L	• Third Party Provider (TPP - incl. fintechs) • Internet-based threat actor • Employee with technical access • IaaS provider employee with technical access • Legitimate user with compromised device • Open Banking service layer provider with technical access (disgruntled employee)	• Anomaly detection with machine learning and/or statistics on data of usage monitoring (ex. Focusing on meta data)
API monitoring and analytics	Lack of logging/monitoring Ex. API10:2019: Insufficient Logging and Monitoring	Exposed APIs	L	M	L	N/A	• Create proper audit trails for all messages received • Ensure APIs provide the necessary level of details in logs to determine the origin of an instruction and submitted call parameters

Dev Sec Ops

Category	Name	Prerequisites	C	I	A	Likely threat agent(s)	Mitigations
Dev Sec Ops	Buggy APIs get to production	N/A	H	M	L	• Third Party Provider (TPP - incl. fintechs) • Internet-based threat actor • Employee with technical access • IaaS provider employee with technical access • Legitimate user with compromised device • Open Banking service layer provider with technical access (disgruntled employee)	• Requirements based on threat landscape • Implement a proper DevSecOps process for building new or changing existing APIs (Security as Code, Infrastructure as Code) • APIs change and evolve fast, so avoid hasty deployments with a well-defined development process and automated tools • Monitor dependencies • Risk based vulnerability management

1.1. Architecture Diagram

The following picture shows a typical API architecture and outlines how these security objectives can be realized using a delegation pattern. On this schema we cover the use case where the financial institution is directly exposing APIs to TPP, without intermediary of an Open Banking service layer provider.

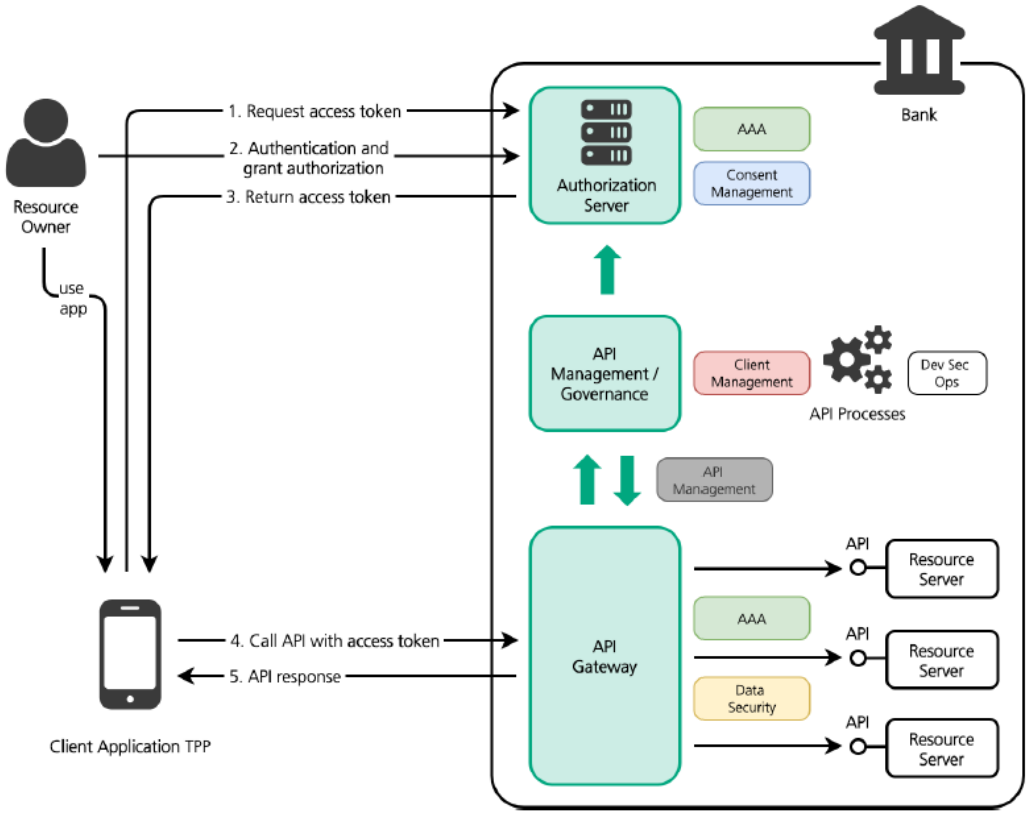


Figure 5: Open API platform

This paragraph outlines what is needed to provide APIs in a secure manner. The definitions in bold here are also visible in the image above.
The access control to APIs is usually realized with a delegation pattern. Delegation in this context means that the user authorizes an application to access its data. This application is often from a third-party provider (TPP) and may use APIs from different organizations. Delegation allows the client application to act on behalf of the user on the API and therefore access the user's data.

It is all about a **client application** that works on services that are available over an API, the so-called **resource servers**.

- The client application calls the API on behalf of a particular person, the so-called **resource owner**.
- To make this possible, the resource owner **grants authorizations** (also called giving consent) on the **authorization server** to the particular client.
- To do this, the authorization server asks the resource owner for **authentication** and to confirm the requested authorizations for the client. Ideally, consent for the user data can be given or withdrawn at any time by the resource owner.
- The authorization server issues an **access token** for the client. The client application can collect this token at the authorization server by authenticating itself (technical user).

All this allows the client application to work on behalf of the resource owner on the resource server according to the granted authorizations. This process is also often called delegation because work with some resources has been delegated.

Since this process has a lot to do with authentication and authorization, the authorization server is often provided by the customer IAM solution (CIAM) of an organization. But it still needs a close integration with the API management suite since the management of the client applications and the APIs is done there.

The recommended protocol to be used for this delegation is OAuth2. OAuth2 enables the client to work on the API on behalf of the resource owner using the OAuth2 access token.

Also concerning access control, the **API gateway** needs to ensure the validity of the access token with each request. Additionally, it checks if the access token contains the authorization needed for the requested API. Furthermore, the API gateway also protects the APIs with traffic limitations and web application firewall features to inspect the requests and their content. This is also the time to collect data for the monitoring of APIs and to detect and react to anomalies such as improper calls and attacks on APIs.

Management and governance of APIs are realized by adding a component to the API gateway, e.g., a portal, a console, and/or programmable interfaces. Tasks such as the registration of new client applications, deploying new APIs or new API versions can be executed with this component. Data collected during run-time on the API gateway also gets processed by this component for monitoring and audit reasons.

A common API suite provides you with all the tools needed to operate a secure API infrastructure. Nevertheless, clear and well-defined API processes concerning design, development, deployment, and decommissioning of APIs are also important for running a secure API platform.

4. Appendix

A.1. Compliance Requirements

Name	Applicability	Summary of main requirements
Regulation (EU) 2016/679 General Data Protection Regulation (GDPR)	Applies to controllers and processors located within the EU or outside the EU if they offer goods or services to, or monitor the behaviour of EU data subjects, as far as their behaviour takes place within the Union. Applies to controllers and processors not established in the EU, but in a place where Member State law applies by virtue of public international law.	Types of personal data - Identify types of personal data collected - Identify sensitive data - Identify data collected from children/whether parental consent is required Data subject information - Inform data subjects of the data processing activities performed that concern them - Inform the data subjects of their rights (access, rectification, objection, erasure) - Inform the data subjects in case of data breach (as well as regulatory authorities) Data processing - Confirm the lawful basis for the processing - Confirm that personal data collected is adequate, relevant and limited to what is necessary for the purpose - Perform a Data Protection Impact Assessment (DPIA) - Apply "privacy by design" and "privacy by default" to solution design - Identify processors; ensure processors comply with applicable GDPR requirements; address in contracts - Maintain records of processing activities Data storage - Determine where and how data is stored - Establish limits for data erasure and periodic reviews - Review data retention policies to ensure data is only kept for as long as necessary

Name	Applicability	Summary of main requirements
		- Establish and/or review processes for rectifying inaccurate data - Prepare for data access requests Data transfers to other countries - Identify data transfers to third countries or international organizations - Assess validity of current mechanisms for personal data transfers - Assess controller-processor agreements Data security - Implement technical and organizational measures to prevent unlawful destruction, loss, alteration, disclosure of/access to personal information - Ensure that processors are employing adequate technical and organizational measures ; address in contracts - Establish and/or update data breach response plan

A.2. Glossary

Term /acronym	Meaning
ISDP concept	Information Security and Data Privacy concept
ToE	Target of Evaluation
SaC	Security as Code
IaC	Infrastructure as Code