

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1149

(05/2020)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Secure applications and services (1) – Web security

Security framework of an open platform for FinTech services

Recommendation ITU-T X.1149

ITU-T X-SERIES RECOMMENDATIONS
DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES (1)	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols (1)	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1360–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1389
Distributed ledger technology security	X.1400–X.1429
Distributed ledger technology security	X.1430–X.1449
Security protocols (2)	X.1450–X.1459
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699
QUANTUM COMMUNICATION	
Terminologies	X.1700–X.1701
Quantum random number generator	X.1702–X.1709
Framework of QKDN security	X.1710–X.1711
Security design for QKDN	X.1712–X.1719
Security techniques for QKDN	X.1720–X.1729
DATA SECURITY	
Big Data Security	X.1750–X.1759
5G SECURITY	X.1800–X.1819

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1149

Security framework of an open platform for FinTech services

Summary

Recommendation ITU-T X.1149 describes an open platform architecture for financial technology (FinTech) services. It also specifies threats and vulnerabilities of open platform, open application programming interface (API) usage procedure for FinTech services, and detailed security requirements to open platform of FinTech services from both financial company and FinTech company sides. The appendix to this Recommendation includes some use cases of the proposed open platform.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1149	2020-05-29	17	11.1002/1000/14250

Keywords

FinTech, open API, open platform.

* To access the Recommendation, type the URL <http://handle.itu.int/> in the address field of your web browser, followed by the Recommendation's unique ID. For example, <http://handle.itu.int/11.1002/1000/114250>.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2020

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

		Page
1	Scope	1
2	References.....	1
3	Definitions	1
	3.1 Terms defined elsewhere	1
	3.2 Terms defined in this Recommendation.....	1
4	Abbreviations and acronyms	2
5	Conventions	2
6	Overview	3
	6.1 FinTech and security	3
	6.2 Open platform.....	3
7	Reference architectures for FinTech services.....	4
	7.1 Architecture of digital financial service provided by traditional financial companies	4
	7.2 Architecture with FinTech service providers	4
	7.3 Open platform for FinTech services.....	5
8	Threats and vulnerabilities of open platform.....	6
	8.1 Threats	6
	8.2 Vulnerabilities	9
9	Open API usage procedure for FinTech services	10
10	Security requirements for open platform of FinTech services	11
	10.1 Security requirements to financial companies.....	11
	10.2 Security requirements to FinTech companies	15
	Appendix I – Use cases of open application programming interface	24
	I.1 Useful points about APIs.....	24
	I.2 Use cases (business models) using open APIs	24
	Bibliography.....	27

Introduction

FinTech revolution has been one of increasing interest in the last few years. It has disrupted the status quo of financial industry, modernized legacy financial institutions, and changed the way consumers access financial products and services. As FinTech start-ups grow in number and sophistication, they are establishing an increasing number of links with traditional financial institutions. However, interfaces between systems are a common source of cybersecurity vulnerabilities, often caused by mismatched configurations and parameters of the systems being connected.

This Recommendation provides an open platform architecture to identify threats and vulnerabilities of interfaces among financial companies, FinTech companies and users, and specifies security requirements for FinTech services to enhance competitiveness of the financial industry to offer diversified users' options.

Recommendation ITU-T X.1149

Security framework of an open platform for FinTech services

1 Scope

This Recommendation provides a security framework for an open platform that supports financial technology (FinTech) services.

This Recommendation demonstrates the evolution of the FinTech service platform to an open platform, analyses threats and vulnerabilities of open platform and open application programming interface (API), describes an open platform architecture and an open API usage procedure for FinTech services, and specifies detailed security requirements for FinTech services. Appendix I of this Recommendation describes use cases of the open platform API.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 open standards [b-ITU-T L.1370]: Standards made available to the general public and which are developed (or approved) and maintained via a collaborative and consensus driven process.

NOTE – Open standards facilitate interoperability and data exchange among different products or services and are intended for widespread adoption.

3.1.2 patch [b-ITU-T X.1206]: A broadly released fix for a product-specific, security-related vulnerability. A method of updating a file that replaces only the parts being changed, rather than the entire file.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 access key: A string issued by an authorization server to access the protected resources hosted by the resource server.

NOTE – In an open platform, the financial technology (FinTech) company requests the access key issued by the financial company in order to access the resources of the financial company.

3.2.2 financial technology (FinTech): ICT technologies used by a financial industry to improve financial services. FinTech includes the applications, processes, products, or technology models in the financial services industry, composed of one or more financial technologies that are provided as an end-to-end process via the Internet.

NOTE – This definition is based in part on the information found in [b-FinTech].

3.2.3 open application programming interface (API): A publicly available application programming interface (API) that provides developers with programmatic access to a proprietary software application or web service.

NOTE – This definition is based in part on the information found in [b-OAPI].

3.2.4 open platform: A software system which is based on open standards [b-ITU-T L.1370], such as published and fully documented external application programming interfaces (APIs) that allow using the software to function in other ways than the original programmer intended, without requiring modification of the source code. Using these interfaces, a third party could integrate with the platform to add functionality.

NOTE – This definition is based in part on the information found in [b-OPLTM].

3.2.5 platform: A hardware or software system that serves as a foundation or base for realizing a certain functionality.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API	Application Programming Interface
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
CEO	Chief Executive Officer
CISO	Chief Information Security Officer
CVE	Common Vulnerabilities and Exposures
DMZ	Demilitarized Zone
FinTech	Financial Technology
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
I/F	Interface
ICT	Information and Communication Technology
IT	Information Technology
PaaS	Platform as a Service
SEO	Search Engine Optimization
SMS	Short Message Service
SQL	Structured Query Language
URL	Uniform Resource Locator

5 Conventions

This Recommendation uses the following conventions:

The keywords "**is required to**" indicate a requirement which must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.

The keywords "**is recommended**" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

The keywords "**is prohibited**" indicate a requirement which must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.

In this Recommendation, the words "**shall**", "**shall not**" and "**should**" may sometimes appear, in which case they are to be interpreted, respectively, as "**is required to**", "**is prohibited**" and "**is recommended**". The appearance of such phrases or keywords in an appendix or in material explicitly marked as informative are to be interpreted as having no normative intent.

6 Overview

6.1 FinTech and security

Digitalization is transforming the financial industry into an ultra-competitive market. Traditional high-street financial companies are scrambling to implement digital transformation projects to become more agile to meet challenges like aggressive time-to-market, fierce competition for customers and shifting business models from product-centric to user-centric. Traditional financial companies have difficulties handling users' diverse needs and personalized services by themselves with their limited human and technology resources, thus there is a market vacuum for innovative FinTech services provided by FinTech companies. Start-up FinTech companies have to overcome obstacles to interconnect to various existing financial companies in order to provide comparable service capabilities with even smaller workforces and access to testbeds to validate their initial products based on real and sufficient data. Therefore, there is a need for an open platform to exchange and integrate data and services from existing financial companies to test FinTech products.

Developers from both financial and FinTech companies use open APIs to connect technologies (mostly apps, but also platforms and systems) to create digital financial innovations. APIs provide open connections between platforms. Failure to protect these connections will give hackers the opportunity to attack API services with either stolen or invalid credentials. Financial services must not overlook the security risk associated with the creation of financial apps in the open platform environment – in particular, API security.

6.2 Open platform

In computing, an open platform describes a software system that is based on open standards [b-ITU-T L.1370], such as published and fully documented external APIs that allow additional functions in ways other than the original programmer intended, without requiring modification of the source code. Using these interfaces, a third party could integrate with the platform to add functionality.

Using an open platform, a developer could add or alter features or functionalities that other platform vendors did not complete or did not envision, as its specifications are publicly available as open standards.

Generally, a platform is a hardware or software system that serves as a foundation or base for realizing a certain functionality on top of it. In case of software platforms, they offer a set of services that facilitate application development when used. According to the definition of 'open platform' in clause 3.2.4, a software platform could be called 'open' if it has one or more of the following characteristics, as highlighted in [b-ReAAL]:

- open API (ref. 3.2.2): An open API that is well documented and publicly available for use by application developers;
- open scope (extensibility): Extensibility refers to the capability of using the platform for purposes for which it was not originally planned;
- open source: Open source refers to the availability of software source code, in a given programming language, in which a license gives licensees freedom to study, change and distribute the software according to the license agreement. There are different open source licensing models with different degrees of freedom for change, usage, and distribution of the software in source code or binary forms. An open platform does not mean it must be open

source, however most open platforms have APIs in open source implementations, resulting in open source platforms. Open source platforms do however always provide open APIs;

- open usage (adoptability): Adoptability refers to enabling others to use the open platform while bypassing specific business development negotiations. This does not necessarily mean that the usage has to be royalty-free;
- open adaptation (adaptability): Assuming that its specifications are publicly available, adaptability of an open platform refers to the possibility of 'changing' an existing functionality of the platform itself, as opposed to 'adding' a new functionality.

7 Reference architectures for FinTech services

7.1 Architecture of digital financial service provided by traditional financial companies

Figure 1 illustrates a traditional functional architecture for digital financial services. In this architecture every financial company has developed and operated financial services and provides its own apps, user can connect directly to financial companies and must use different apps of individual financial companies for same services.

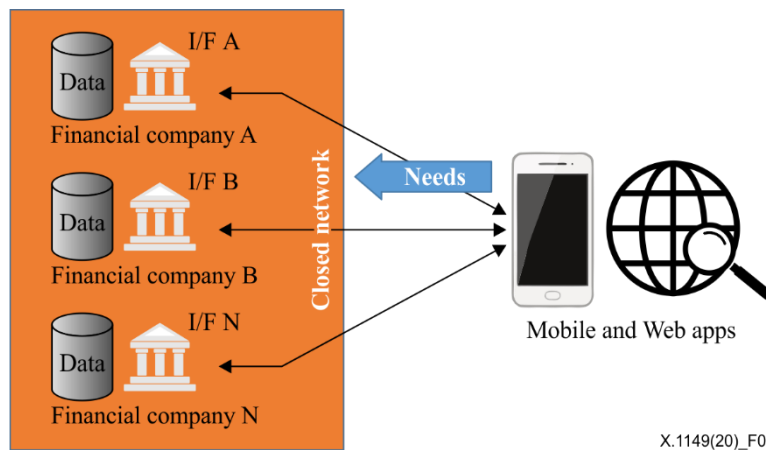


Figure 1 –Architecture of digital financial services provided by traditional financial companies

7.2 Architecture with FinTech service providers

Due to the rapid development of information and communication technology (ICT), it is difficult for financial companies to develop and operate on their own the financial services they provide to users. As FinTech companies have better ICT techniques and capabilities, financial companies want to use those FinTech companies to handle the difficulties and to obtain a competitive edge when compared to their competitors.

Figure 2 shows an architecture with emerged FinTech service providers, which are not in the architecture of traditional digital financial services. Financial companies hire different FinTech companies to develop different service apps and provide respective APIs for them. This architecture allows a financial company to provide users with respective apps for each of its services. This architecture causes inconvenience to users that a user has to connect to different apps of each financial company interface. This architecture has a characteristic of limited data sharing, which is the data of a financial company that is opened to a FinTech company so that the FinTech company has a dedicated authorization to access a user's data in this financial company, but the FinTech company has no authorization to access data of the same user in other financial companies. Whenever the FinTech company accesses the user's data beyond agreement with the origin financial company, it must obtain permission or authorization. Users interact differently and in a non-standardized manner

with each of the FinTech companies. FinTech companies must secure each of its interfaces with each financial company and user.

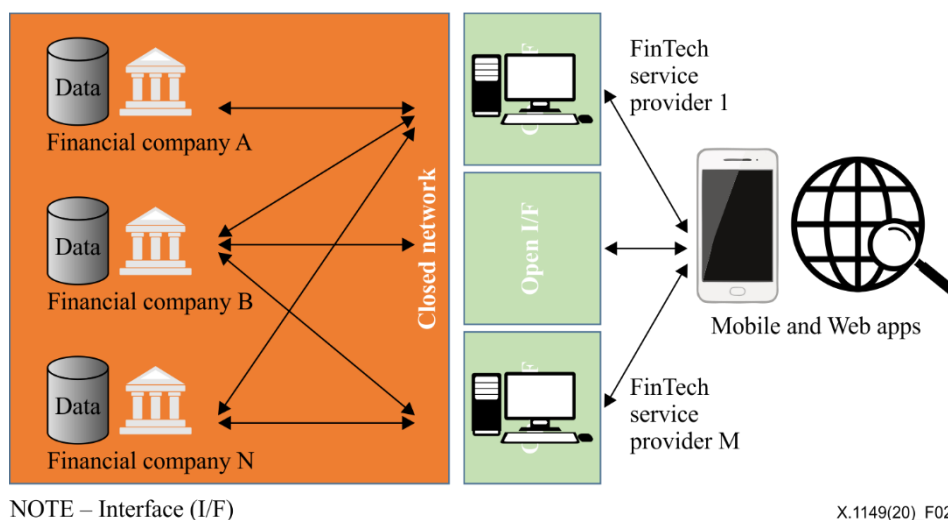


Figure 2 –Architecture with FinTech service providers

7.3 Open platform for FinTech services

As discussed in the architecture with FinTech service providers (Figure 2), usability and efficiency to provide financial services are two problematic issues. On one hand, a FinTech company needs additional permissions across financial companies to integrate and create new data and services. On the other hand, the interfaces of the FinTech with different financial companies are different among themselves.

An open platform with open APIs in a standardized format provides an efficient interface for using open APIs, a common place to create and share value-added data and services using users' data located among financial companies, and serves as a testbed for new services and open APIs. Figure 3 shows an open platform architecture for FinTech services to streamline third-party data access and use secure open APIs to protect data and services for users.

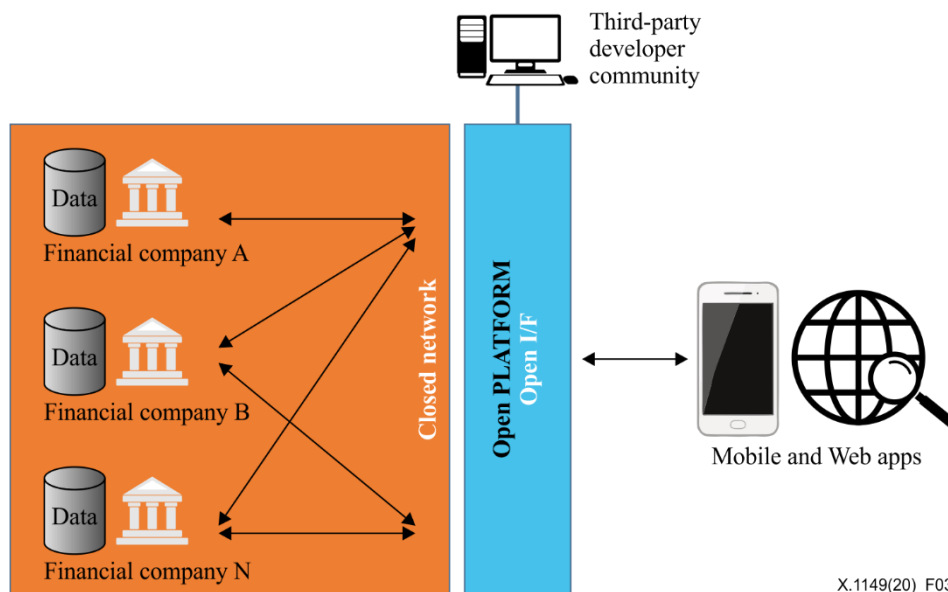


Figure 3 – Open platform architecture for FinTech services