Fiorano

A Guide to Open Banking Acronyms

Everything you wanted to know about Open Banking but didn't know whom to ask

A

B

C

E

F

H

I

J

M

N

O

P

Q

R

S

T

U

Z

Introduction

Open Banking is now mainstream and showing no sign of stopping. The UK's Open Banking regime crossed its 5th anniversary on 13th January 2023. With more than 6.5 million active users, the UK has set the world's template for Open Banking, Open Finance, and broader, secure customer-consented Open Data sharing.

As the GCC, Jordan, and Canada embrace Open Banking, banks have little time to implement the essential technology to publish Open Banking APIs in a secure format.

Open Banking introduces a plethora of acronyms unfamiliar to most bank CxOs. We felt it an appropriate time to update this essential acronyms self-help guide which we originally released in 2018 for Open Banking in the UK.

A

AIS

Account Information Services – an online service that provides consolidated information on payment accounts held by a payment service user with Payment Service Providers. In the UK, PSD2 will bring existing payment service providers under the scope of the regulation and ensure that AISPs (See AISP) can receive access to payment accounts while also placing requirements on them to provide security for users.

AISP

Account Information Service Provider – Organisations registered under a specific country's relevant CA / NCA to provide AIS services or who have passport-ed into a different host country CA / NCA to provide AIS services (See CA / NCA).

A

API

Application Programming Interface – A set of software functions and procedures that allow the creation of applications that access the features or data of an operating system, application, or another service. From a PSD2 standpoint, while the RTS does not explicitly specify the use of APIs for banks to promote and control data sharing, APIs are the only long-term and sustainable method to deliver XS2A elegantly.

ASPSP

Account Servicing Payment Service Provider – The legal entity providing and maintaining a payment account for a payer as defined by the PSRs, and in the context of the open banking ecosystem, are the entities that publish Read/Write APIs to permit payments initiated by Third Party Account Information or Payment Initiation Service Providers via API endpoints.

B

Berlin Group

A pan-European payments interoperability harmonisation in the initiative and technical standardisation body, with the primary objective of defining open and common scheme- and processor-independent standards in the inter-banking domain.

The Berlin Group currently has participation from 25 major players in the payments industry from 10 different Euro-zone countries and the UK, Sweden, Denmark, Norway, Iceland, Turkey, Bulgaria, Hungary, Serbia, and Switzerland, together representing more than 25 billion card-originated transactions annually within the Single Euro Payments Area (SEPA). For PSD2, the Berlin Group has worked on a detailed "Access to Account Framework' with a data model at conceptual, logical, and physical data levels and associated messaging based on the EBA RTS.

CA / NCA

Competent Authority / National Competent Authority for consumer protection – the national authority competent for the protection of consumer rights when dealing with credit or financial institutions in each EU Member State. As a trusted source, NCAs also may publish an NCA Public Register as a standard and secure service for validation of TPP's regulatory access levels by ASPSPs. The CA for the United Kingdom is the FCA. A list of CAs' websites, categorised by country, is provided here.

CBPII

Card-Based Payment Instrument Issuer - for PSD2, CBPIIs sit alongside AISPs and PISPs as Payment Services Providers. CBPIIs can request confirmation from an ASPSP on whether a customer has funds available in their account to complete a transaction at a given time, and ASPSPs must provide a yes or no answer. Banks / ASPSPs need to ensure their systems and processes are in place to respond to requests from CBPIIs within a very short timescale, even for accounts in which the ASPSP itself may not be offering cards.

CMA 9

Based on the volume of personal and business current accounts, the nine largest banks and building societies in Great Britain and Northern Ireland. The CMA 9 set up and funded the OBIE based on an order by the CMA in 2016.

CMA

Competition & Markets Authority (UK) is a London headquartered, independent non-ministerial department that promotes competition for the benefit of consumers both within and outside the UK.

CN

Subject Common Name - the Software Statement ID (SSID) for the software statement for which the certificate has been created.

CRL

Certificate Revocation Lists – One of two commonly accepted mechanisms to check the validity of Trust certificates such as eIDAS, the other being the Online Certificate Status Protocol to check the validity of a certificate in real-time. While OCSP is considered the most accurate approach, real-world latency and network load considerations often result in CRLs being chosen, essentially a list of revoked certificates.

CSC

Common and Secure Communication - specifications for safeguarding the confidentiality and integrity of data to ensure the security of communication sessions between ASPSPs, AISPs, PISPs, and CBPIIs. The RTS for SCA and CSC comes under Article 98 of the PSD2.

CSR

Certificate Signing Request - Once a Software Statement has been created, a CSR is required for ASPSPs and TPPs to sign requests and create digital certificates to encrypt messages over the public network.

CVM

Customer Verification Method – used for verifying customers (e.g., using signatures) during card payment transactions.

EBA

The European Banking Authority is an independent EU authority working to ensure effective and consistent prudential regulation and supervision across the European banking sector, along with the European Securities and Markets Authorities (ESMA) and the European Occupational Pensions Authority (EIOPA).

EC

European Commission

ECDSA

Elliptical Curve Digital Signing Algorithm - A request object signing algorithm supported by Open Banking.

eIDAS

The electronic Identification Authentication & Trust Services Regulation is an EU regulation that sets out rules for electronic identification and trust services. It refers to a range of services that help verify the identity of individuals and businesses online or the authenticity of electronic documents. In the PSD2 context, banks and TPPs use Qualified Certificates for websites and Qualified Certificates for Electronic Seals, which QTSPs will issue based on the ETSI TS 119 495 standards published in May 2018. Qualified certificates will include unique numbers such as URN/GURN to identify payment institutions and an entity's NCA. Along with APIs and SCA, eIDAS is technically required to be part of the access mechanisms ASPSPs need to implement and make available to TPPs, in time for the September 2019 timeline. All TSPs are bound by Article 13 of the eIDAS to provide clear limitations for which their trust services may be used and to assume liability for any damage caused intentionally or negligently or a failure to comply with the eIDAS.

ERPB

Euro Retail Payments Board – the legal entity under the European Central Bank set up in 2013 to replace the SEPA Council and develop an integrated, innovative, and competitive market for retail payments in the EU. It is an ERPB Working Group on PIS which recently highlighted practical gaps in the RTS regarding PSD2 interfaces and other elements.

ETSI TS 119495

Electronic Signatures and Infrastructures Technical Specifications; Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements specifies profiles of qualified certificates for electronic seals and website authentication to be used by payment service providers under the PSD2 for providing evidence with legal assumptions of authenticity (including identification and authentication of the source) and integrity of a transaction.

ETSI

An independent recognised European standards body and not-for-profit organisation, dealing with telecommunications, broadcasting, and other electronic networks and services. The ETSI supports European regulations and legislation by creating harmonised European Standards. Along with other European Standards Organisations (ESOs), CEN, and CENELEC, the ETSI is the only other ESO whose standards are recognised as European Standards.

ETV

Exempted Threshold Value, related to SCA, refers to a specific amount electronic transactions should not exceed to qualify as low-risk and hence exempt from SCA.

EU 2015/2366

Directive of the European Parliament and of the Council on 25th 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.

EU 2018/389

Commission Delegated Regulation (EU) 2018/389 of 27th November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and the Council with regards to technical regulatory standards for strong customer authentication and common and secure open standards of communication.

FAPI OP

FAPI OpenID Providers, certified by the OpenID Foundation after demonstrating certification to the FAPI 1.0 Final profile, as either FAPI 1 Advanced Final (Generic), the UK Open Banking profile, the Australia CDR profile, the more recent Brazil Open Banking/Open Insurance profiles, or the FAPI 1.0 Second Implementors draft.

FAPI

Termed initially as Financial-grade APIs: The technical specification developed by the OpenID Foundation and adopted in Open Banking specifications globally to deliver technical API security requirements for the financial industry, with OAuth 2.0 and OpenID Connect (OIDC) as its base.

FCA

The Financial Conduct Authority, the NCA in the UK responsible for enforcing PSD2.

hipTAN

Related to SCA, hipTAN refers to transaction authentication codes received on a chip-enabled security device separate from the PSUs mobile device.

ISO 20022

The ISO standard for APIs in financial services was developed by the International Organisation for Standardisation (ISO) as an established way to build message standards within the financial services industry. ISO 20022 is a common language for all financial communications supporting interoperability between all parties. When APIs are implemented in a cross-industry setting between many institutions with different data sets, ISO 20022 can add value by providing common business data semantics in a standardised and uniform structure.

JARM

JWT secured Authorization Response Mode for OAuth 2.0 enhances the security of the standard authorisation response. In addition to PAR, JARM was one of the main other sets of incremental recommendations incorporated into current OpenID specifications by Brazil for Open Banking & Open Finance.

JSON

The de-facto data exchange standard in most mobile applications, JSON, is intrinsically linked with APIs and is commonly used along with ISO 20022 elements. As an example, Open Banking UK uses both JSON and ISO 20022.

JWKS

JSON Web Key Set - a JSON notation for sharing public keys used to verify the signature of a signed JWT.

JWT

JSON Web Token - an open standard that defines a compact and self-contained way for securely transmitting data between entities as a JSON object. Information contained within a signed JWT can be trusted as they are digitally signed using a secret key pair. TPPs who want to onboard with an ASPSP must generate a TPP registration request JWT which contains the SSA and other claims. In the UK, the JWT is issued and signed by the Open Banking Directory.

M

MATLS

Mutual Authentication TLS - the mechanism used to protect the Open Banking directory Rest APIs and bank endpoints. Third parties must use the transport certificate issued by the OB Directory to exchange an authorisation code for an access token. The ASPSP will ensure that the TLS certificate being used matches that of the OAuth client.

MSCA

Member State Competent Authority – the PSD2 Regulator in each member state, responsible for approving/rejecting TPP applications, issuing Authorisation numbers, and adding authorised TPPs to the country's Home Public Register.

NFC

Near Field Technology – one of the underlying technologies used in mobile devices where payment transactions from PSUs may be initiated. NFC allows devices to talk to each other and is often used in contactless payments.

OAuth / OAuth 2.0

Short for Open Authorization, OAuth is an open standard, delegated authorisation framework for access delegation to REST/APIs used to access protected data within apps/systems through secure delegated access. While both OAuth 1.0 and OAuth 2.0 specifications are active, they are entirely different.

OB / OBUK

Open Banking is a term used to refer to a secure way to give service providers access to an individual's financial information. Open Banking in the UK is designed to bring more competition and innovation to financial services. While the initial scope for Open Banking was mandatory for the CMA9, the OBIE emerged from this to set the standard for PSD2 in the UK.

OBIE

The Open Banking Implementation Entity – the company set up by the CMA in 2016 to deliver Open Banking in the UK. The OBIEs trading name is Open Banking Limited, and its role is to:
(a) Design the specifications for the APIs that banks and building societies (in the UK) use to provide Open Banking and PSD2 securely;
(b) Support regulated TPPs, Banks, and ASPSPs to use the Open Banking standards;
(c) Create security and messaging standards;
(d) Produce guidelines for participants in the Open Banking ecosystem;
(e) Set out the processes for managing disputes and complaints; and
(f) Manage the Open Banking Directory, which allows regulated participants to enroll in Open Banking.

OIDC

Open ID Connect - built on top of the OAuth 2.0 protocol and often used for federated authentication in the context of PSD2, and Open Banking OIDC provides identity tokens. Anyone entering the Open Banking UK ecosystem must be OIDC enabled.

OLO

One Leg Out transactions – Under PSD2, OLO transactions are those where the payer/recipient service provider is based outside the EU. OLO transactions were largely out of scope in the original PSD, as were transactions in non-EU currencies. PSD2 brings all OLO transactions within scope so long as any one of the service providers is in the EU, concerning the parts of the transaction carried out in the EU and all currencies.

OpenID

An Open standard and decentralised identity & authentication protocol (different from the OAuth authorization protocol) promoted by the non-profit OpenID Foundation is used to verify the identity of a user to a client's service. OpenID has been adopted by Open Banking specifications globally (noticeably Open Banking UK and Brazil) as it uses JSON web tokens (JWT) and avoids sharing user credentials with services.

PAR / Illustrated PAR

Pushed Authorization Requests, this extension describes a technique of initiating an OAuth flow from a bank's backchannel instead of a URL, providing better security and more flexibility for a complex authorisation request.

Passport / Passporting

The EBA's RTS on the framework for cooperation and exchange of information between CAs for passport notifications under the PSD2 outlines the format and notification templates to be used between Competent Authorities when a payment institution in one Member State applies to provide services in another Member State via a "Passport" application. This Passport application may be a Branch Passport application, a Services Passport application, or an Agent Passport application.

This is done to enhance cooperation between competent authorities (CAs) and ensure a consistent and efficient notification process for payment institutions intending to exercise the right of establishment and the freedom to provide services on a cross-border basis across the EU.

PIS

Payment Initiation Services – an online service that accesses a user's payment account to initiate the transfer of funds on their behalf with the user's consent and authentication. Payment Initiation Services provides an alternative to paying online using a credit or debit card. PSD2 will ensure that PISPs receive access to payment accounts while also placing requirements on them to provide security for users.

PISP

Payment Initiation Service Provider – Organisations registered under a specific country's relevant CA / NCA to provide PIS services or who have passport-ed into a different host country CA / NCA to provide PIS services.

PSD

The original Payment Services Directive (2007/64/EC) is an EU Directive administered by the European Commission (Directorate General Internal Market) to regulate payment services and payment service providers throughout the EU and EEA. The original PSD's purpose was to increase pan-European competition and participation in the payments industry from non-banks and to provide a level playing field by harmonizing consumer protection and the rights and obligations of payment providers and users.

PSD2

The European Parliament adopted the Revised Directive on Payment Services (EU)2015/2366, commonly known as PSD2, on 8th October 2015 as a step towards a single digital market to benefit consumers and businesses and help the economy grow. On 13th January 2018, Directive 2007/64/EC was repealed and replaced by (EU)2015/2366.

P

PSR

The Payment System Regulator – the economic regulator for the UK's £81 trillion payment systems industry. Together with the UK's FCA, the PSR monitors and enforces the EU's PSD2 in the UK. The term PSR/PSRs is also used to broadly refer to the regulations such as the Payment Services Regulations 2017 (PSRs 2017)

PSU

Payment Services User – the end customer or user (a person) in a PSD2 transaction who makes use of an Account Information (AIS) or Payment Initiation (PIS) service as a payee, payer, or both by providing TPPs access to their bank account.

QSEALC

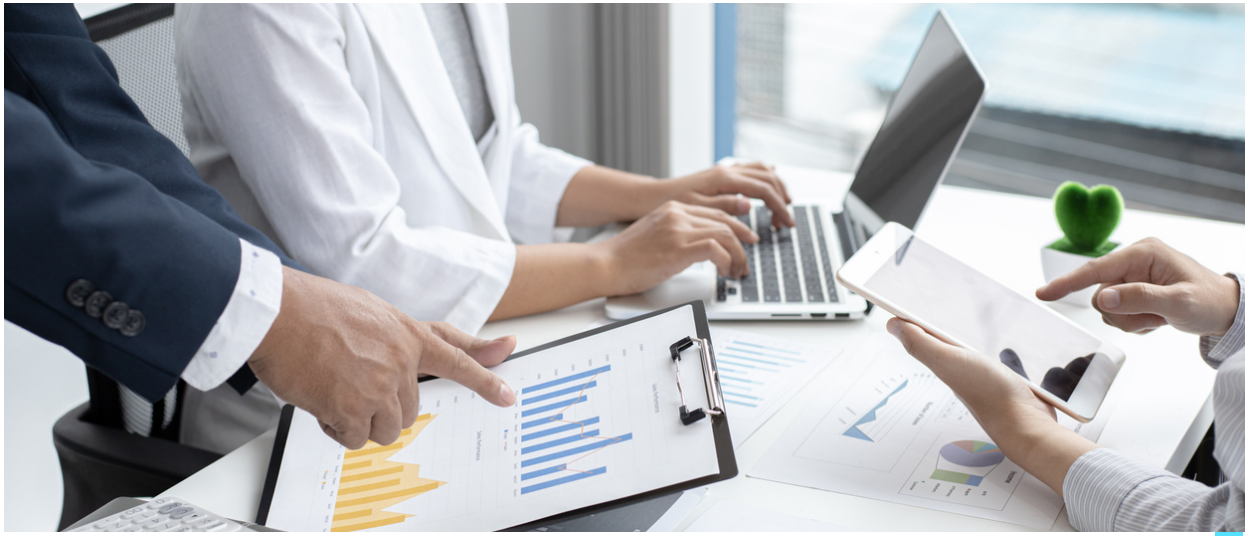
Qualified Electronic Seal Certificates – used at the Application layer, with messages being passed between communicating parties to prove the origin, authenticity, and integrity that the data comes from the party it is meant to. From an SCA/CSC standpoint, QSEALCs can be used to establish the PSD2 'Financial Identity' as opposed to the internet identity in the QWAC.

QWAC

Qualified Website Authentication Certificates – provide a method to authenticate "Internet Entity Identity" and encrypt communications to provide confidentiality. QWACs are used with specific protocols at the Transport layer and are not designed to be used at the Application layer.

RTS

Regulatory Technical Standards – published by the European Banking Authority (EBA) specify various technical requirements (e.g., SCA, CSC, Passporting) that PSD2 players must meet to provide services in a format that is accepted. The formats consider the various objectives of the PSD2, including enhanced security, promoting competition, ensuring technology and business-model neutrality, contributing to the integration of payments in the EU. RTSs are technology and business-model-neutral.



S

S2A

Access2Account – the technical acronym for access to customers' payment accounts by third-party providers (via APIs). Under the XS2A, banks must (through an API format) provide a service exposing customer account information and payment initiation to any third party registered under a Competent Authority and with the consent of the PSU.

SBA

The Slovak Banking Associations standardisation initiative for PSD2.

SCA

Strong Customer Authentication – ensuring customer protection in PSD2 transactions by applying an increased level of security in electronic payments. SCA is to be used under certain conditions as defined in the PSD2 RTS:
(a) When a customer (individual or corporate) accesses their payment account online (including just an aggregated view);
(b) When making an electronic payment; and
(c) When carrying out any action through a remote channel that may imply a risk of payment fraud or other abuses.

In practice, SCA will be applied using mechanisms to check a customer's identity using at least any two of the following:
(i) Knowledge
(ii) Possession
(iii) Inherence
The specification requires a unique authentication code to be used, which dynamically links the transaction to a specific amount and a specific payee. The RTS also lists several possible exemptions to SCA to try and keep electronic payments as convenient and seamless as possible.

S

smsTAN

Also related to SCA and sometimes referred to as SMS OTP (One Time Password), smsTAN refers to transaction authentication codes received via the SMS channel on the PSU's mobile device.

SSA

Software Statement Assertion - A JSON Web Token (JWT) containing client metadata about an instance of TPP client software. ASPSPs must not accept client registration requests that do not include a valid SSA. ASPSPs are required to provide the following:
(i) a service that can validate and process a request JWT and the SSA JWT it receives from TPPs, supporting both the PS256 and ES 256 of all types;
(ii) service to create and return client credentials based on the security characteristics obtained from metadata;
(iii) Storing the Software Statement ID from the SSA against the client and validating the TPP, App, and SSID.org jwks_endpoint;
(iv) a discovery specification endpoint that confirms with the OIDC discovery specification advertising supported mechanisms and algorithms available to TPPs.

STET

STET S.A. – headquartered in France, is a European leader in payments processing (SIPS) and is owned by six major banks – BNP Paribas, BPCE, Crédit Agricole, Banque Fédérative du Crédit Mutuel, La Banque Postale, and Société Générale. STET actively contributes to European discussions and efforts to provide the market with harmonised payment solutions. From a PSD2 standpoint, STET is one of the competing standards or guidelines vying for dominance against the Berlin Group and Open Banking UK. It is, however, interesting to note that STET is one of the key participants of the Berlin Group.

TLS

Transport Layer Security protocol works hand-in-glove on the network layer, with OAuth 2.0 at the application layer. TLS goes beyond standard SSL protocols to secure connections by encrypting traffic and validating the authenticity of counterparties. SSL and TLS are cryptographic protocols that provide authentication and data encryption between servers, machines, and applications.

TPP

Third-Party Providers – Organisations that use APIs developed to standards to access customers' accounts to deliver Account Information or Payment Initiation related Services. TPPs may be either AISPs or PISPs, or both. See AISP and PISP.

TRA

Transaction Risk Analysis - method for analysing risk levels associated with associated PSD2 transactions. The ETV is linked to corresponding fraud rate categories under PSD2 specific TRA.

TSP / QTSP

Trust Service Providers (TSPs) are commercial organisations or government entities that provide digital services which enable the issuance and proving mechanisms to secure information from official sources and protect it against tampering in transit, allowing Trust. A Qualified status (hence QTSP) is awarded to TSPs who undergo national accreditation under eIDAS through a written Conformity Assessment. The Qualified status is intended to provide the European Market with a reliable standard that ensures a basic level of confidence when choosing a Trust service supplier; it also guarantees a level of interoperability across the European Trust infrastructure. Each EU Member State regulates QTSPs under an appointed Member State Supervisory Body (MSSB).

All TSPs are bound by Article 13 of the eIDAS to provide clear limitations for which their trust services may be used and to assume liability for any damage caused intentionally or negligently or a failure to comply with the eIDAS.

URN / GURN

Unique Reference Number / Global Unique Reference Number – a unique code combining Country + NCA code + an entity's registration number to uniquely identify a payment institution within a public registry. The unique authorisation number may contain a PSD header to differentiate PSD identifiers and could take the format of:

PSD - <Country_Code> - <Home NCA > - <Entities_number_in_the_registry>

ZBP

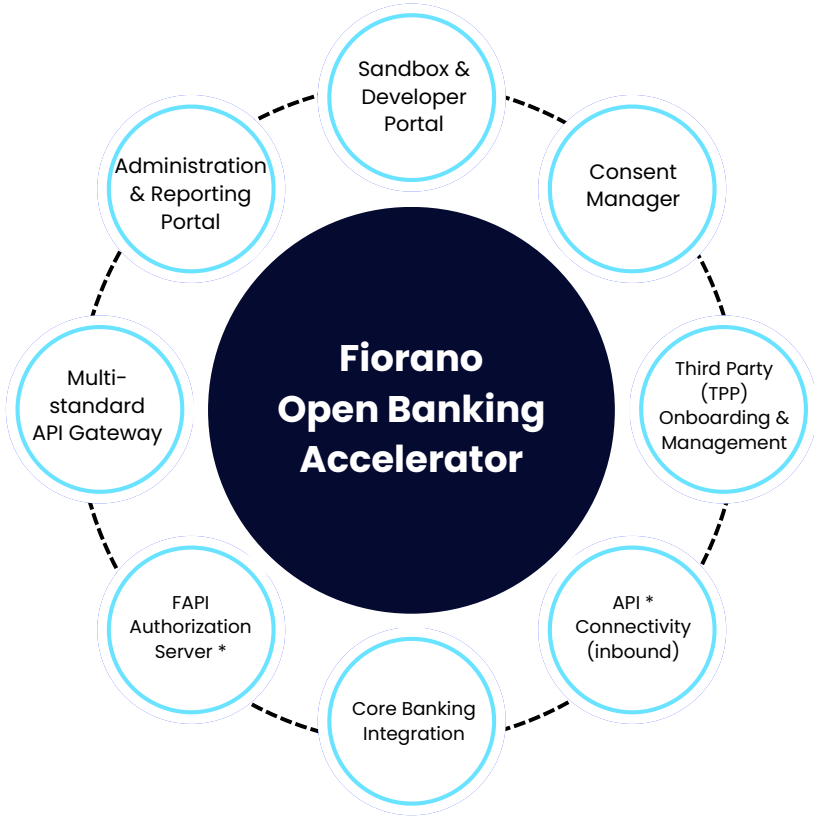
The Polish Bank Association initiative for PSD2, spearheaded by the Polish Banking Federation.

Fiorano Open Banking Accelerator

Fiorano's Open Banking Accelerator has been in production in the UK since 2019 and has matured through multiple global Open Banking API publishing specifications, including OBIE (UK), Berlin Group, NextGen PSD2, BCB and FDX.

The platform delivers everything a bank needs to comply quickly with Open Banking API publishing mandates and provides several extensions / add-ons to help Financial Institutions monetise Open Banking.

Fiorano's Open Banking Accelerator is full-coverage, supporting all deployment models



For more details on how Fiorano can help accelerate your Open Banking plans, contact us at: info@fiorano.com

ABOUT FIORANO

Enabling Change at the Speed of Thought

Fiorano is a cloud-native event-streaming microservice composition platform that powers the next generation of digitally enabled real-time enterprises.

By making business operations event-driven, the Fiorano Platform allows companies to improve customer experiences and quickly adapt to fast-changing market conditions.

Fiorano operates worldwide through its offices in multiple countries and network of partners across the globe.

Drop us a line:

info@fiorano.com