1 Table of Contents

2 GDPR Compliance on PRISMA Application Server (PRISMA AS/PRISMA) 2

2.1 Abstract 2

3 Prisma Application Server 2

3.1 PRISMA Application Server Arch 3

4 General Data Protection Regulation Overview 3

4.1 Changes the GDPR Introduces to Organizations Operating in the EU 3

4.2 PRISMA AS Preparation for the GDPR 4

4.3 PRISMA AS Data Processing Addendum (DPA) 4

4.4 The Role of PRISMA AS Under the GDPR 4

4.4.1 PRISMA Application Server as a Data Processor 4

4.4.2 PRISMA Application Server as a Data Controller 5

4.5 Shared Security Responsibility Model 5

5 Strong Compliance Framework and Security Standards 5

5.1 PRISMA AS Compliance Program 5

6 The CISPE Code of Conduct 6

7 Data Access Controls 6

7.1 PRISMA AS Identity and Access Management 7

7.2 Multi-Factor-Authentication 7

7.3 Captcha 7

7.4 Access to PRISMA AS Data 7

7.5 Defining Boundaries for Services Access 7

8 Monitoring and Logging 7

8.1 Compliance Auditing and Security Analytics 9

8.2 Collecting and Processing Logs 9

8.3 Centralized Security Management 10

9 Protecting your Data on Prisma Application Server 10

9.1 No data are stored on disk 10
9.2 SQL Server Transparent Data Encryption (TDE) 11
9.3 Encrypt Data in Transit 11
9.4 PRISMA AS Service Integration 11
9.5 Integration with Prisma Application Services and Third-Party Applications 11
9.6 Open Data 11
9.7 Data Protection by Design and by Default 12
10 Contacts 12
11 Contributors 13
12 Document Revision 13

2 GDPR Compliance on PRISMA Application Server (PRISMA AS/PRISMA)

2.1 Abstract

This document provides information about services and resources that PRISMA AS offers customers to help them align with the requirements of the General Data Protection Regulation (GDPR) that might apply to their activities.

These include adherence to IT security standards, adherence to the Cloud Infrastructure Services Providers in Europe (CISPE) Code of Conduct, data access controls, monitoring and logging tools, encryption, and key management.

3 Prisma Application Server

PRISMA is a web application framework and, more specific, a software platform designed to support the development of internet applications and services.

PRISMA provides clear and easily manageable structures, allowing rapid and consistent development of all the critical aspects of a web application:

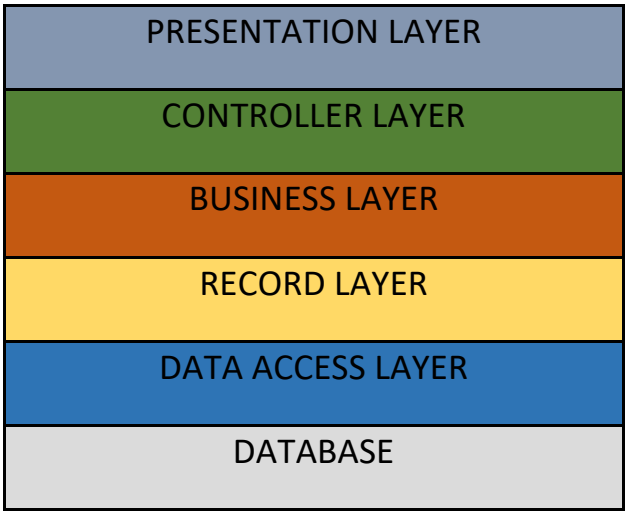
- Don’t repeat yourself (DRY)
- Keep it short and simple (KISS)

- Convention over Configuration

3.1 PRISMA Application Server Arch

PRISMA AS is built on client / server architecture in which the functional process logic, data access, data storage in the server and the user interface are developed and managed as independent modules on separate layers.

The three-tier architecture is a software design model and an established architecture that allows it to be scaled and adapted over time.



4 General Data Protection Regulation Overview

The General Data Protection Regulation (GDPR) is a European privacy law (Regulation 2016/679 of the European Parliament and of the Council of April 27, 2016) that became enforceable on May 25, 2018. The GDPR replaces the EU Data Protection Directive (Directive 95/46/EC) and is intended to harmonize data protection laws throughout the European Union (EU) by applying a single data protection law that is binding throughout each EU member state.

The GDPR applies to all processing of personal data either by organizations that have an establishment in the EU, or to organizations that process personal data of EU residents when offering goods or services to individuals in the EU or monitoring the behavior of EU residents in the EU. Personal data is any information relating to an identified or identifiable natural person.

4.1 Changes the GDPR Introduces to Organizations Operating in the EU

One of the key aspects of the GDPR is that it creates consistency across EU member states on how personal data can be processed, used, and exchanged securely. Organizations must demonstrate the security of the data they are processing and their compliance with the GDPR on a continual basis, by

implementing and regularly reviewing technical and organizational measures, as well as compliance policies applicable to the processing of personal data.

4.2 PRISMA AS Preparation for the GDPR

PRISMA AS compliance, data protection, and security experts work with customers to answer their questions and help them prepare to run workloads in the cloud under the GDPR. These teams also review the readiness of PRISMA AS against the requirements of the GDPR.

4.3 PRISMA AS Data Processing Addendum (DPA)

PRISMA AS offers a GDPR-compliant Data Processing Addendum (GDPR DPA), which enables customers to comply with GDPR contractual obligations.

The PRISMA AS GDPR DPA is incorporated into the PRISMA AS Service Terms and applies automatically to all customers globally who require it to comply with the GDPR.

On 16 July 2020, the Court of Justice of the European Union (CJEU) issued a ruling regarding the EU-US Privacy Shield and Standard Contractual Clauses (SCCs), also known as “model clauses.” The CJEU ruled that the EU-US Privacy Shield is no longer valid for the transfer of personal data from the European Union (EU) to the United States (US). However, in the same ruling, the CJEU validated that companies can continue to use SCCs as a mechanism for transferring data outside of the EU.

4.4 The Role of PRISMA AS Under the GDPR

Under the GDPR, PRISMA AS acts as both a data processor and a data controller.

Under Article 32, controllers and processors are required to “...implement appropriate technical and organizational measures” that consider “the state of the art and the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons”. The GDPR provides specific suggestions for what types of security actions may be required, including:

- The pseudonymization and encryption of personal data.

- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.

- The ability to restore the availability and access to personal data in a timely manner, in the event of a physical or technical incident.

- A process to regularly test, assess, and evaluate the effectiveness of technical and organizational measures to ensure the security of the processing.

4.4.1 PRISMA Application Server as a Data Processor

When customers use PRISMA AS Services to process personal data in their content, PRISMA AS acts as a data processor.

Under these circumstances, the customer may act as a data controller or a data processor, and PRISMA AS acts as a data processor or sub-processor.

4.4.2 PRISMA Application Server as a Data Controller

When PRISMA AS collects personal data and determines the purposes and means of processing that personal data, it acts as a data controller.

For example, when PRISMA AS processes account information for account creation, administration, data access, or contact information for the PRISMA AS account to help through customer support activities, it acts as a data controller.

4.5 Shared Security Responsibility Model

Security and Compliance is a shared responsibility between PRISMA AS and the customer.

When customers move their data to the cloud, security responsibilities are shared between the customer and the cloud service provider.

When customers move they data to the PRISMA Application Server, PRISMA AS is responsible for protecting data from unwanted for all of the services exposed from PRISMA Application Server.

Customers and Partners, acting either as data controllers or data processors, are responsible for anything they put in the PRISMA AS or connect to the PRISMA Application Server.

This differentiation of responsibility is commonly referred to as security of the cloud versus security in the cloud.

This shared model can help reduce customers' operational burden and provide them with the necessary flexibility and control to deploy their infrastructure in the PRISMA Application Server.

The shared responsibility model is a useful approach to illustrate the different responsibilities of PRISMA AS (as a data processor or sub-processor) and customers or Partners (as either data controllers or data processors) under the GDPR.

5 Strong Compliance Framework and Security Standards

According to the GDPR, appropriate technical and organizational measures might need to include "the ability to ensure the ongoing confidentiality, integrity, availability and resilience of the processing systems and services," as well as reliable restore, testing, and overall risk management processes.

5.1 PRISMA AS Compliance Program

PRISMA AS continually maintains a high bar for security and compliance across all our global operations.

Security has always been our highest priority.

PRISMA AS regularly undergoes independent third-party attestation audits to provide assurance that control activities are operating as intended.

More specifically, PRISMA AS is audited against a variety of security frameworks.

6 The CISPE Code of Conduct

- The GDPR contemplates the approval of codes of conduct to help controllers and processors demonstrate compliance under the regulation. One such code that is awaiting official approval from EU data protection authorities is the CISPE Code of Conduct for Cloud Infrastructure Service Providers (the Code). The CISPE Code of Conduct helps cloud customers ensure that their cloud infrastructure provider is using appropriate data protection standards to protect their data consistent with the GDPR. The following are a few key benefits of the Code:

Clarifies who is responsible for which aspects of data protection–The Code explains the role of both the cloud provider and the customer under the GDPR, specifically within the context of cloud infrastructure services.

- Defines the principles providers must follow–The Code develops key principles in the GDPR about clear actions and commitments that providers should undertake to demonstrate their compliance with GDPR and help customers comply. Customers can use these concrete benefits in their own compliance and data protection strategies.

- Gives customers the privacy and security information necessary to help them achieve their compliance goals – The Code requires providers to be transparent about the steps they are taking to deliver on their privacy and security commitments. A few of these steps include the implementation of privacy and security safeguards, notification of data breaches, data deletion, and transparency

of third-party sub-processing. All these commitments are verified by third party, independent monitoring bodies. Customers can use this information to fully understand the high levels of security provided.

7 Data Access Controls

Article 25 of the GDPR states that the controller “shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed”.

The following PRISMA AS access control mechanisms can help customers comply with this requirement by allowing only authorized administrators, users, and applications to get access to PRISMA AS and customer data.

7.1 PRISMA AS Identity and Access Management

PRISMA uses a flexible, secure modular authentication system.
Internal authentication requires the user to be authenticated through the framework while external authentication is delegated to other user repositories.
Each individual user managed by the system can use different authentication providers.

PRISMA authentication works with cryptographic algorithm. In case of external providers, the passwords are not stored locally but reside directly on the external authentication service.

PRISMA implements standard authentication modules for LDAP / OpenLDAP, Italian SPID etc.

For proprietary or not directly supported systems, it is possible to extend the authentication system with .NET modules.

7.2 Multi-Factor-Authentication

For extra security, you can add two-factor authentication to your PRISMA AS account. With multi-factor authentication (MFA) enabled, when you sign into the Prisma Application Server, you are prompted for your username and password (the first factor), as well as an authentication response from your PRISMA AS MFA device (the second factor, google or Microsoft authenticator).

7.3 Captcha

For extra security you can enable Captcha validation provided by google re-captcha.

7.4 Access to PRISMA AS Data

To implement granular access to your PRISMA AS data, you can grant different levels of permissions to different users for different data types.

For example, you can allow only some users to read data only for their country.

7.5 Defining Boundaries for Services Access

IT – Information Technologies Srl does not access or use your content for any purpose without your consent. All our services are located in italy or EU.

8 Monitoring and Logging

Article 30 of the GDPR states that "...each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility". This article also includes details about which information must be recorded when you monitor the processing of all personal data. Controllers and processors are also required to send breach notifications in a timely manner, so detecting incidents quickly is important.

To help enable customers to comply with these obligations, PRISMA AS offers the following monitoring and logging services:

- Web Server Access log
- Database log
- Prisma Application Log / Prisma Access Log
- Prisma History Log (List of all user actions)
- Custom logs
- Email Notifications, for example when user:
    - Create object
    - Edit object
    - Delete object
    - Custom operation

Results | Messages

	ID	OBJID	STEP	DTE	CONTEXT	MSG
1	1	d395777795404bce9c988584...	637038911239432610	2019-09-12 13:18:43.940	OptimizerSQL	SELECT CAST(EncryptByPassPhrase('prisma','id='+CONVERT(v...
2	2	d395777795404bce9c988584...	637038911239672528	2019-09-12 13:18:43.960	OptimizerSQL	CREATE VIEW V_PRISMA_CMP_d395777795404bce9c98858...
3	3	d395777795404bce9c988584...	637038911240312411	2019-09-12 13:18:44.023	OptimizerSQL	SELECT * FROM V_PRISMA_CMP_d395777795404bce9c9885...
4	4	d395777795404bce9c988584...	637038911241231913	2019-09-12 13:18:44.117	OptimizerSQL	SELECT D52d11d99d7e64f88bdf2255645fd53fe.deleted AS DE...
5	5	d395777795404bce9c988584...	637038911241411877	2019-09-12 13:18:44.133	OptimizerSQL	CREATE VIEW V_PRISMA_OPT_d395777795404bce9c98858...
6	6	d395777795404bce9c988584...	637038911243151250	2019-09-12 13:18:44.310	BaseService::OK::LoadDocument()	SELECT D52d11d99d7e64f88bdf2255645fd53fe.deleted AS DE...
7	7	7dfc7d70cd6e47528eb130c1...	637038911951054177	2019-09-12 13:19:55.127	OptimizerSQL	SELECT CAST(EncryptByPassPhrase('prisma','id='+CONVERT(v...
8	8	7dfc7d70cd6e47528eb130c1...	637038911951154174	2019-09-12 13:19:55.137	OptimizerSQL	CREATE VIEW V_PRISMA_CMP_7dfc7d70cd6e47528eb130c1...
9	9	7dfc7d70cd6e47528eb130c1...	637038911951624059	2019-09-12 13:19:55.183	OptimizerSQL	SELECT * FROM V_PRISMA_CMP_7dfc7d70cd6e47528eb130...
10	10	7dfc7d70cd6e47528eb130c1...	637038911951774037	2019-09-12 13:19:55.197	OptimizerSQL	SELECT D2f7f80f8ef5f48d7aa378daf5cab5d17.deleted AS DEC...
11	11	7dfc7d70cd6e47528eb130c1...	637038911951844042	2019-09-12 13:19:55.203	OptimizerSQL	CREATE VIEW V_PRISMA_OPT_7dfc7d70cd6e47528eb130c1...
12	12	7dfc7d70cd6e47528eb130c1...	637038911952673829	2019-09-12 13:19:55.287	BaseService::OK::LoadDocument()	SELECT D2f7f80f8ef5f48d7aa378daf5cab5d17.deleted AS DEC...

Figure 1 - Prisma Query Log

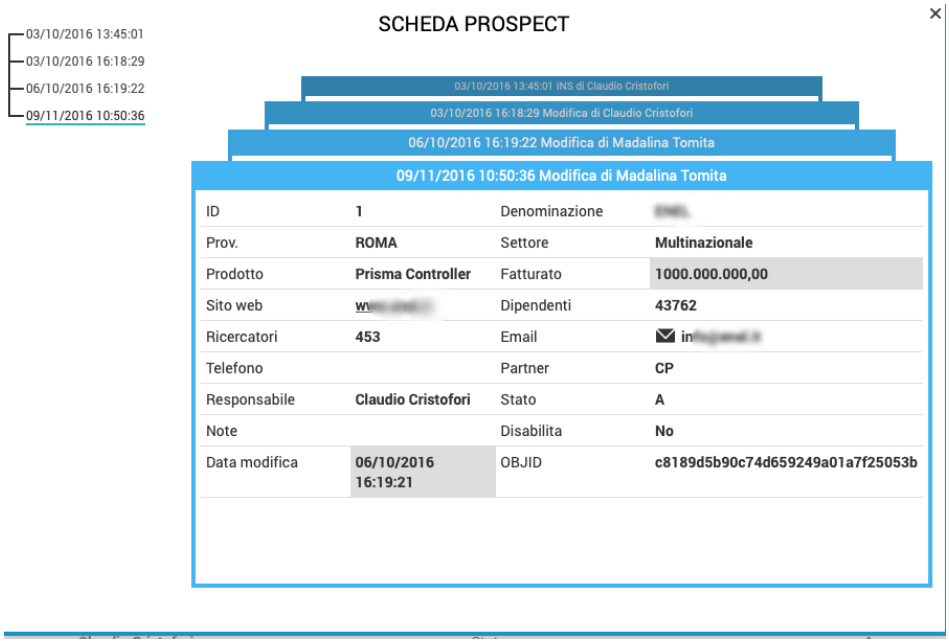


Figure 2 - Data History

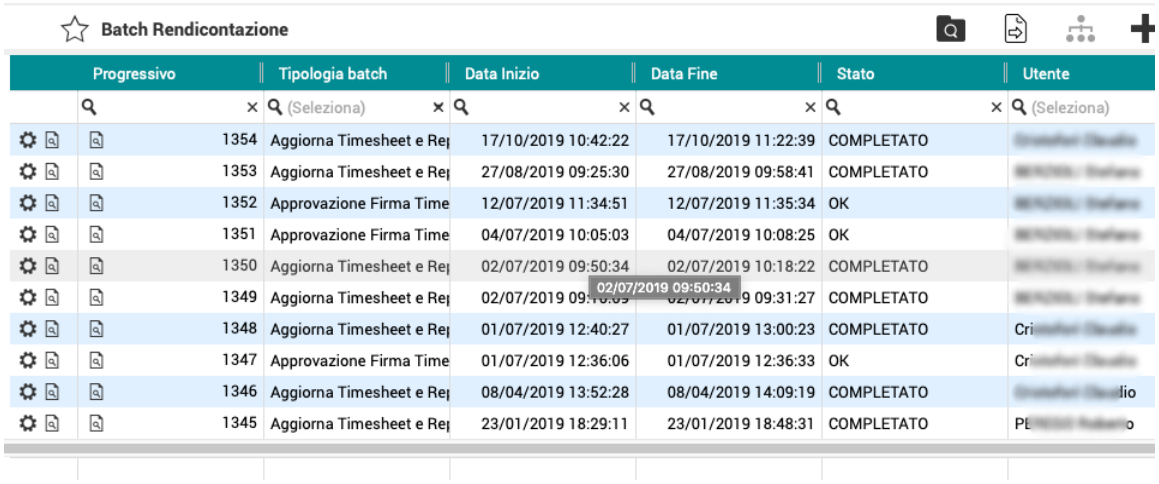


Figure 3 - Custom Log

8.1 Compliance Auditing and Security Analytics

With PRISMA AS, you can continuously monitor account activity. A history of the API calls is captured, including API calls made through the Application itself, running batch, sql execution, type of entities requested, …

Log can also be aggregated and exported to other systems for analysis. Standard format are supported json, xml, plain text, …

8.2 Collecting and Processing Logs

Prisma Log can be used to monitor, store, and access your log files from Prisma Application Server.

Logs information includes, for example:

- Granular logging of access to Prisma Entities
- Detailed information about all type of flows
- Rule-based configuration verification and actions with Prisma Roles Manager

Logs can be analyzed interactively using Prisma Logs, performing queries to help you respond more efficiently and effectively to operational issues.

8.3 Centralized Security Management

Many organizations have challenges related to visibility and centralized management of their environments.

As your operational footprint grows, this challenge can be compounded unless you carefully consider your security designs.

Lack of knowledge, combined with decentralized and uneven management of governance and security processes, can make your environment vulnerable.

PRISMA AS provides identity management using Azure Single Sign-On default directory and enables cross-account audit using Microsoft Azure.

PRISMA AS also provides LDAP authentication and customizable authentication plugin modules.

9 Protecting your Data on Prisma Application Server

Article 32 of the GDPR requires that organizations must "...implement appropriate technical

and organizational measures to ensure a level of security appropriate to the risk, including ...the pseudonymization and encryption of personal data[...]". In addition, organizations must safeguard against the unauthorized disclosure of or access to personal data."

Encryption reduces the risks associated with the storage of personal data because data is unreadable without the correct key. A thorough encryption strategy can help mitigate the impact of various security events, including some security breaches.

9.1 No data are stored on disk

PRISMA AS doesn't store any sensitive data in the file system. All data are stored in Microsoft SQL Server and configurations are database based.

9.2 SQL Server Transparent Data Encryption (TDE)

Transparent Data Encryption (TDE) encrypts the data within the physical files of the database, the 'data at rest'. Without the original encryption certificate and master key, the data cannot be read when the drive is accessed, or the physical media is stolen. The data in unencrypted data files can be read by restoring the files to another server.

9.3 Encrypt Data in Transit

Prisma Applications Server support HTTPS endpoints using the TLS protocol for communication, which provides encryption in transit when you use Prisma Dashboard Application, Prisma Application REST API and Webservices.

9.4 PRISMA AS Service Integration

Every IT Team knows the crucial importance of the widest and most automatic integration possible of the data stored in the various systems available to the company: ERP, CRM, Database, Mainframe, File, Web Services, etc.

Prisma allows to connect to different systems and data providers, under a single dashboard, implementing a single access point to all distributed data, new or existing, with secure https.

9.5 Integration with Prisma Application Services and Third-Party Applications

Prisma can be configured to expose application services via Webservices or Rest API.

All requests from service consumers are logged by PRISMA by default.

9.6 Open Data

Open data are information resources that the user, the company or a community freely decides to make available to third parties, partially, totally or with restrictions.

PRISMA allows you to publish (make accessible via Open Data) its dataset feeds in a fully automatic way and through free file formats (CSV, XML, JSON, etc.).

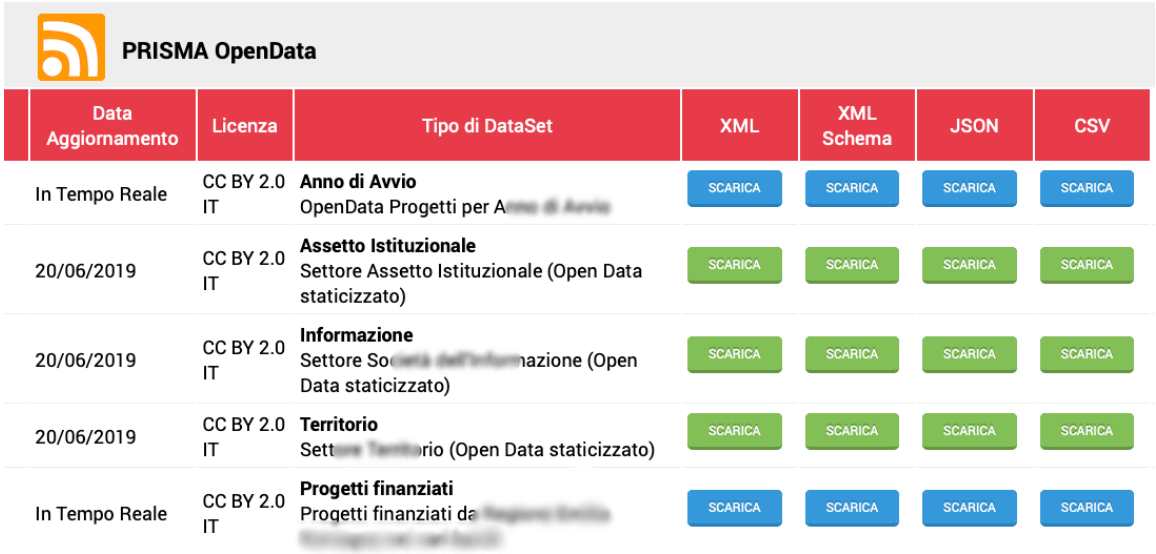


Figure 4 - Open Data

All requests from service consumers are logged by PRISMA by default.

9.7 Data Protection by Design and by Default

Any time a user or an application tries to use the Prisma AS Dashboard, the Prisma AS API a request is sent to Prisma Framework.

The Prisma AS service receives the request and executes a set of several steps to determine whether to allow or deny the request,

according to a specific policy evaluation logic.

Except for admin credential requests, all requests on Prisma AS are denied by default (the default deny policy is applied).

This means that everything that is not explicitly allowed by the policy is denied.
In the definition of policies and as a best practice, Prisma AS suggests that you apply the least privilege principle, which means that every user must be able to access only the resources required to complete its tasks.

This approach aligns with Article 25 of the GDPR, which states that “the controller shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed”.

10 Contacts

IT – Information Technologies Srl

Via Ferrarese, 219/7 – 40128 Bologna – Italy

Email: info@itechnologies.it

Phone: +39 051 223414 - +39 051 6562284

11 Contributors

Contributors to this document include:

Andrea Blè, Technology & solutions Manager

Christian Avanzo, Prisma Solution Architect

Claudio Cristofori, Project Manager

12 Document Revisions

Date	Description
September 2019	First publication
July 2021	Updated to include new services