A CANON COMPANY

Security White Paper

Version: PRISMAdirect 1.4

Copyright and Trademarks

Copyright

Language

Original instructions that are in British English.

Trademarks

Table of content

Foreword 5

1 What is PRISMAdirect 6
1.1 PRISMAdirect and its environment 6
1.2 PRISMAdirect and its components 9
1.3 Use cases 11
1.3.1 Customers 12
1.3.2 Order Managers 13
1.3.3 Operators 14
1.3.4 Approver 14
1.3.5 Administrator 15
1.3.6 JDF Client 15
1.3.7 Outlook Email Client 16
1.4 PRISMAdirect services and accounts 16
1.5 Configurations of PRISMAdirect and its deployment 18

2 System security 20
2.1 Security assessment 20
2.2 Programming languages and technology 20
2.3 Antivirus software, proxy servers and web filter servers 20

3 Network security 21
3.1 PRISMAdirect server 22
3.2 Remote web server 24
3.3 License server 25
3.4 Order processing workstation 26
3.5 Client PC 26
3.6 Diagram of the protocols and ports 21

4 Access control 27

5 Data and data security 28
5.1 Data at rest 28
5.2 Data in transit 28
5.2.1 Web browser 28
5.2.2 File hosting services 29
5.2.3 Import service 30
5.2.4 Export service 30
5.2.5 Scan link 31
5.2.6 Outlook AddIn 31
5.2.7 JDF compatible submitter using JDF/JMF endpoints 31
5.2.8 Web Bootstrap 32

5.2.9 LDAP server 33
5.2.10 Email server 34
5.2.11 PRISMAproduction 34
5.2.12 Printers 34
5.2.13 Payment providers 35
5.2.14 Service provider for tax calculation 37
5.2.15 Shipping providers 38
5.2.16 uniFLOW 39
5.2.17 Océ Remote Service 40
5.2.18 PRISMAprepare 40
5.2.19 Web driver 40
5.2.20 Screen saver 41
5.2.21 License server 41
5.2.22 SQL server 41

6 Appendix 44
6.1 Web Bootstrap 44
6.2 uniFLOW 44

Foreword

This document describes the security features of PRISMAdirect. It discloses which data PRISMAdirect handles and how its security works.
Firstly, this document provides an overview of PRISMAdirect. Secondly, it details all security related issues. For example, which data the application handles and which network protocols and ports are used.

IT administrators are the target group for this security white paper.

Canon can deliver this document to sales companies worldwide. Sales companies can edit the contents of the document before disclosing any of the information to customers.

1 What is PRISMAdirect

PRISMAdirect serves as a:

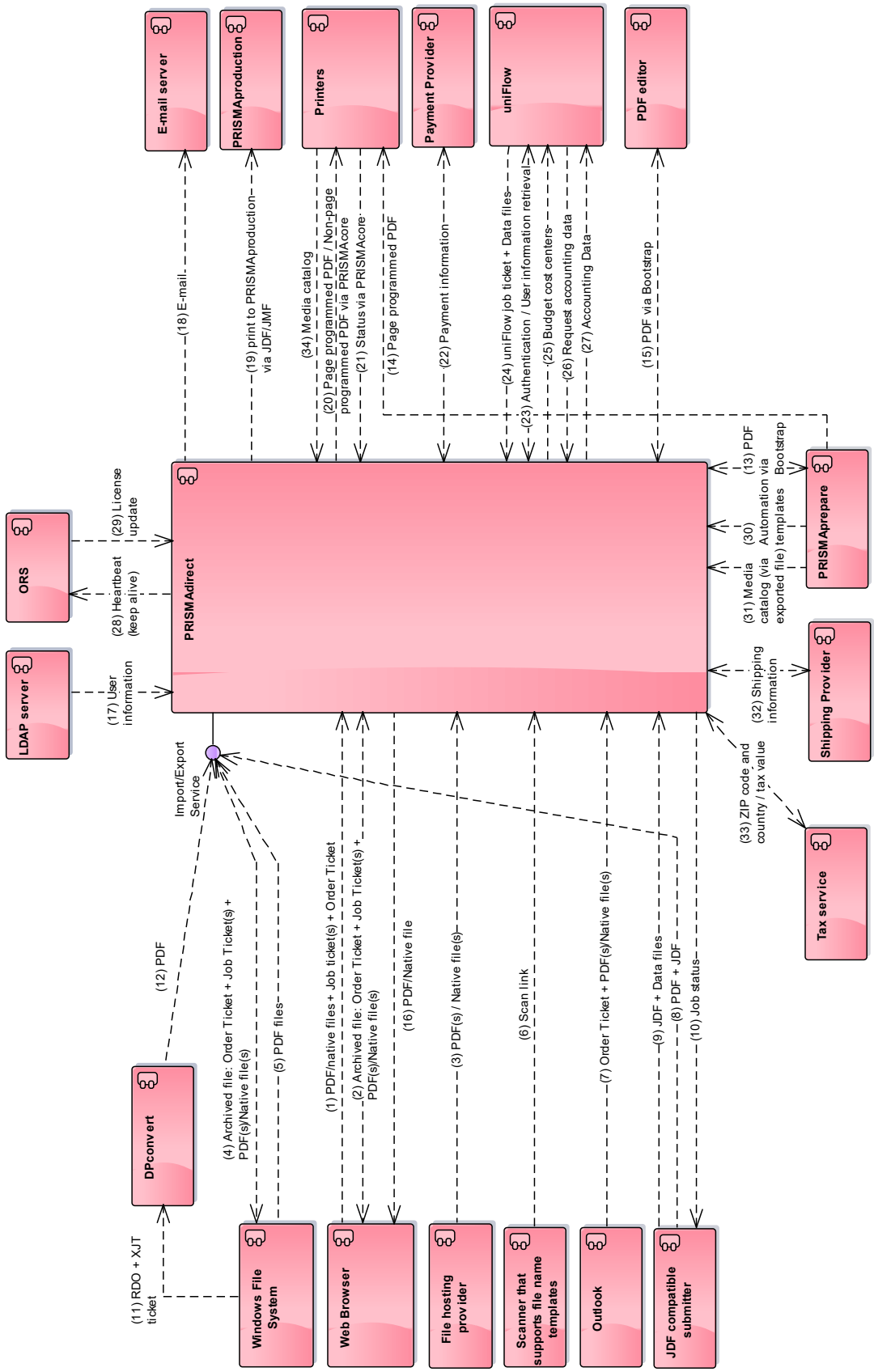
- Web shop / order submission client for the end user
- Order management / production workflow solution for the print room operator.

The PRISMAdirect product targets both the corporate and the commercial printing environment.

PRISMAdirect can be sold together with PRISMAprepare for document preparation. An interface exists between these two products. Documents submitted to PRISMAdirect can be page programmed and printed using PRISMAprepare.

1.1 PRISMAdirect and its environment

PRISMAdirect is a client-server application. The following diagram illustrates the interactions between PRISMAdirect and its environment. Most of the entities of the environment can be located inside or outside the LAN where the server resides.


E-mail server
PRISMAproduction
Printers
Payment Provider
uniFlow
PDF editor
(18) E-mail
(19) print to PRISMAproduction via JDF/JMF
(34) Media catalog
(20) Page programmed PDF / Non-page programmed PDF via PRISMAcore
(21) Status via PRISMAcore
(14) Page programmed PDF
(22) Payment information
(24) uniFlow job ticket + Data files
(23) Authentication / User information retrieval
(25) Budget cost centers
(26) Request accounting data
(27) Accounting Data
(15) PDF via Bootstrap
ORS
(29) License update
(28) Heartbeat (keep alive)
LDAP server
(17) User information
PRISMAdirect
(13) PDF Automation via Bootstrap
(30) Media catalog (via exported file) templates
PRISMAprepare
(31) Shipping information
Shipping Provider
(33) ZIP code and country / tax value
Tax service
Import/Export Service
(12) PDF
(4) Archived file: Order Ticket + Job Ticket(s) + PDF(s)/Native file(s)
(5) PDF files
(1) PDF/native files + Job ticket(s) + Order Ticket
(2) Archived file: Order Ticket + Job Ticket(s) + PDF(s)/Native file(s)
(16) PDF/Native file
(3) PDF(s) / Native file(s)
(6) Scan link
(7) Order Ticket + PDF(s)/Native file(s)
(9) JDF + Data files
(8) PDF + JDF
(10) Job status
DPconvert
(11) RDO + XJT ticket
Windows File System
Web Browser
File hosting provider
Scanner that supports file name templates
Outlook
JDF compatible submitter

The data interactions in the diagram contain numbers enclosed by round brackets. The numbers match the data transmitted between the PRISMAdirect server and its components in the text below.

PRISMAdirect and the web browser transmit data during a number of operations:
- Submit an order that contains one or more jobs with one or more files and tickets (1).
- Add files (1) to existing jobs.
- Import an archive file (2) to create an order. An archive file can contain files and tickets.
- Download the files (16) of each job.

PRISMAdirect can retrieve files for new and existing jobs from file hosting services (3). The file hosting services are outside the LAN where the PRISMAdirect server resides.

PRISMAdirect can create orders directly from the file system using the import service:
- Import an archive file (4) to create an order. An archive file can contain files and tickets.
- Import PDF files (5) using a default ticket.
- The DPconvert module can convert Xerox RDO archive files (11) into PDF files (12). The import service can import the PDF files.

The configured import folder is a hot folder.

PRISMAdirect can export orders (4) to the file system using the export service. The user that runs the export service must have access rights to the export folder, e.g. on a network share.

Scanned jobs can be received through the scan link (6).

Customers can submit one or more files via Outlook. The operator can create an order from the files using the Outlook AddIn. PRISMAdirect imports the order (7) from Outlook.

A JDF compatible submitter can submit:
- A PDF file and a JDF ticket (8) to the import service. This is an optional submission method.
- A JDF ticket and one or more files (9) to the server. This is the default submission method.
- Each change in the job status (10) is sent to the JDF compatible submitter.

A JDF compatible submitter is any application that complies to the JDF standard.

PRISMAdirect can open a number of external applications when you install the web bootstrap. The web bootstrap can download a file for editing and then upload it again into the system.
- The web bootstrap executable allows the operator to page program a PDF file (13) using PRISMAprepare.
- The web bootstrap executable allows the operator to edit a PDF file in a PDF editor, e.g. Adobe Acrobat (15).
- The Print Bootstrap Service synchronizes the automation templates (30).

PRISMAdirect can retrieve available user information (17) from a LDAP server.

PRISMAdirect uses an email server to automatically send email messages (18) on specific events. For each event, a specific email template is used.
Optionally, PRISMAdirect can send jobs to PRISMAproduction using the printer driver of PRISMAproduction (19). The communication is one-way only. No status information is sent back from PRISMAproduction to PRISMAdirect.

PRISMAdirect can send page programmed and non-page programmed PDF files (20) to the printers and receive status information (21). Also, PRISMAprepare can send page programmed PDF files (14) directly to the printers.

PRISMAdirect sends and receives payment information (22) to/from a number of payment providers. The payment providers are outside the LAN where the PRISMAdirect server resides.

PRISMAdirect can be integrated (paired) with uniFLOW. Before pairing, the required ports must be open, or forwarded when the servers are in different LANs. After pairing, PRISMAdirect passes a public key to the JDF Framework. The JDF Framework handles the user authentication on behalf of PRISMAdirect. The uniFLOW server behaves like an LDAP sever.

- A user with rights to the budget management workflow logs in to PRISMAdirect. PRISMAdirect sends the concerning authentication information (23) to uniFLOW. uniFLOW sends available user information (23) pertaining to the budget management workflow back to PRISMAdirect.
- PRISMAdirect can receive jobs (24) from uniFLOW. A job consists of a uniFLOW job ticket and files.
- PRISMAdirect can update the cost centers managed by uniFLOW with budget information (25).
- PRISMAdirect can request accounting data (26) from uniFLOW.
- PRISMAdirect can send accounting data (27) to uniFLOW.

PRISMAdirect sends a heartbeat (28) to Océ Remote Service (ORS) to check the connection. Upon request by the administrator, ORS pushes license updates (29) to PRISMAdirect.

The media catalogue of PRISMAprepare can be exported to a file. PRISMAdirect can import the media catalogue using this file (31).
PRISMAdirect can import the media catalogue (34) from PRISMAsync controllers and EFI controllers.

PRISMAdirect sends and receives shipping information (32) to/from a number of shipping providers. The shipping providers are outside the LAN where the PRISMAdirect server resides.

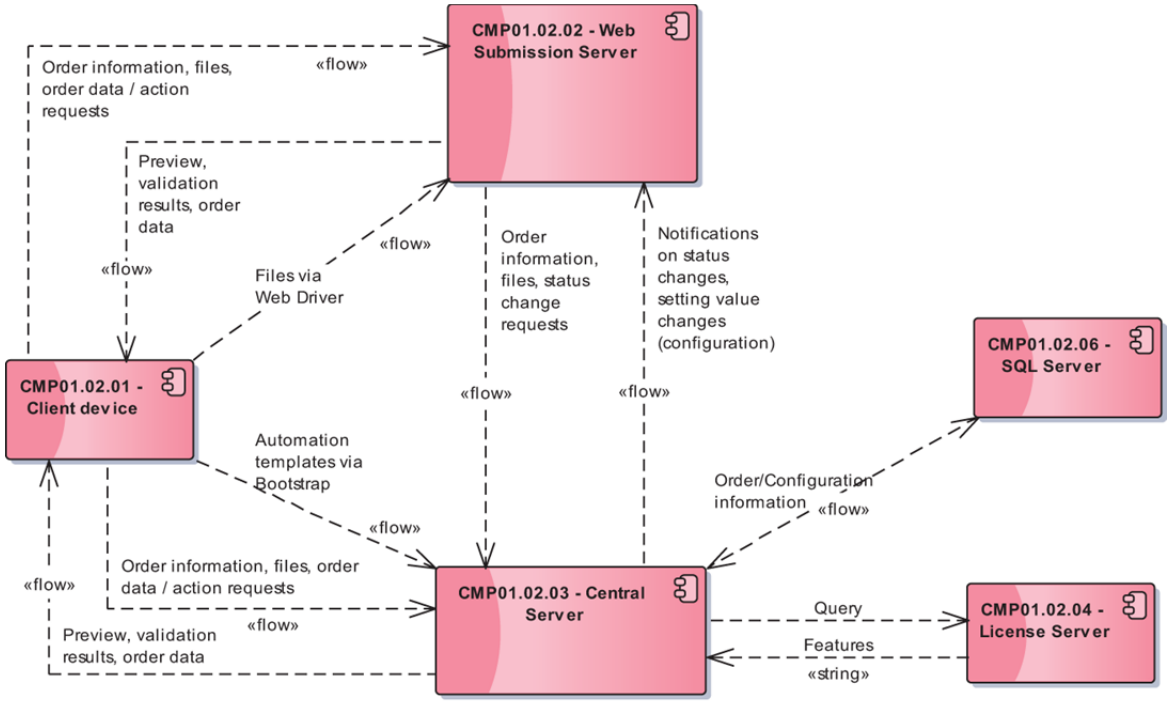
PRISMAdirect sends and receives tax information (33) to/from a service provider for tax calculation. The service provider for tax calculation is outside the LAN where the PRISMAdirect server resides.

1.2 PRISMAdirect and its components

The components of PRISMAdirect can be installed on different computers. The computers containing the components of PRISMAdirect can be inside or outside the LAN where the PRISMAdirect server

resides. For example, when a web server is outside the LAN of the PRISMAdirect server, it is also called a remote web server.

The following diagram illustrates the interactions between PRISMAdirect and its components. Each component can send and receive data and/or responses. The descriptions detail which data and/or responses are sent by each component.



Client device

The client device can be:

- A tablet or a smartphone. These devices can only access the web shop and the order processing console via a web browser.
- A computer which can access all components.

The web browser on the client device connects to:

- Component "Web server" to access the web shop.
- Component "Server" to access the order processing console.

The web browser can send data and requests to component “Server” and component “Web server”:

- Files, tickets and requests, e.g. generate preview for VDP documents.

When PRISMAprepare and the web bootstrap are installed on the client device:

- Automation templates are synchronized from the client device to component “Server”.

The web driver on the client device can send files to the component “Web server”.
The PRISMAdirect configuration can contain one or multiple client devices.

Web server
The web browser on the client PC connects to component "Web server" to access the web shop.
Component “Web server” can send:

- Files, preview information and validation results, e.g. validation of VDP files to the web browser.
- Files, tickets and requests to change the job state to component “Server” when an order is submitted or changed.

The PRISMAdirect configuration can contain none, one or multiple "Web server" components.
Multiple web servers provide load balancing and failover.

Server
Component “Server” can send:

- Files, preview information and validation results, e.g. validation of VDP files to the web browser.
- Job state changes and updated values of settings to component “Web server” when these values are changed in workspace “Configuration”.
- Orders and the configuration settings of PRISMAdirect to the SQL server.
- A request for license information to component “License server”.

The PRISMAdirect configuration contains one "Server" component.

SQL server
The SQL server

- Stores the following data:
  - Job-related metadata
    A set of ticket fields - not the complete ticket - for performance and filtering reasons.
  - PRISMAdirect configuration
  - Cost centers configuration and status, approval workflow status
  - Accounting data and related information
  - Payment history
- Sends the orders and the configuration settings to component “Server”.

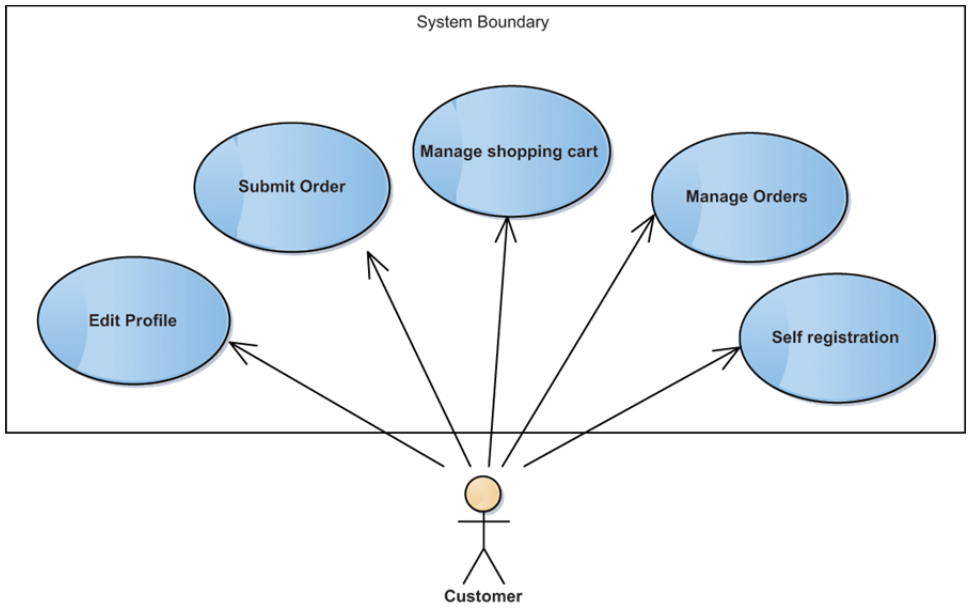
The PRISMAdirect configuration contains one SQL server. PRISMAdirect can install and use a new SQL server. PRISMAdirect can also connect to a SQL server already used by the customer.

License server
Component “License server” sends a string containing the licensed features to component “Server”.
The PRISMAdirect configuration contains one "License server" component.

1.3 Use cases

The use cases describe the interactions between actors and the system to achieve a goal. The human actors are: Customers, Order Managers, Operators, Product Administrator, and Approver. A non-human actor is the JDF Client that uses the JDF/JMF interface to interact with PRISMAdirect.

1.3.1 Customers

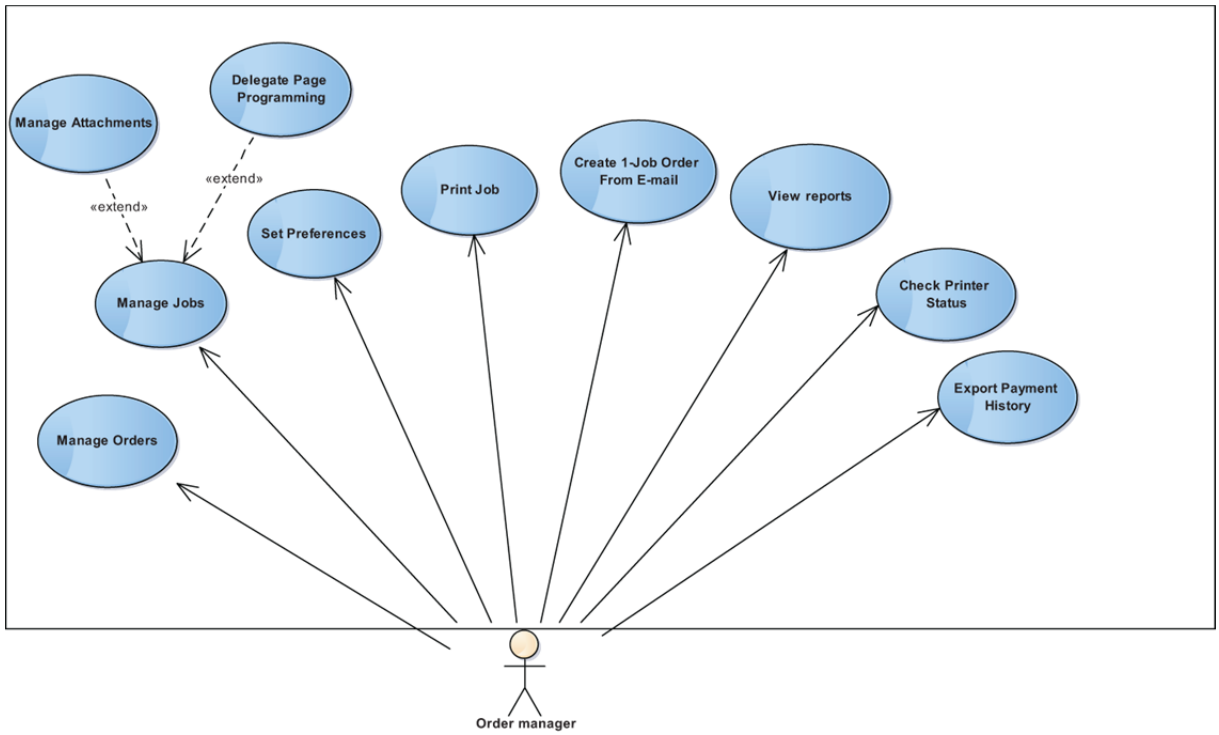


In the web shop, the Customer has access to a shopping cart where items can be added and submitted for production and delivery. The submission of one or more items creates an order in the system containing one or more jobs.

The Customer:

- Has to log in to the system;
- Can manage the orders, including: list the orders, select one or more orders, delete one or more orders, create an order;
- Can manage the jobs inside a selected order, including: list the jobs, select one or more jobs, delete one or more jobs, edit a job;
- Can manage the shopping cart with jobs, prior to submitting an order;
- Can submit orders that contain one or more jobs. Each job can contain one or more files, or no file when stationery is ordered.
- Can edit the profile
- Can register in order to receive access to the web shop.

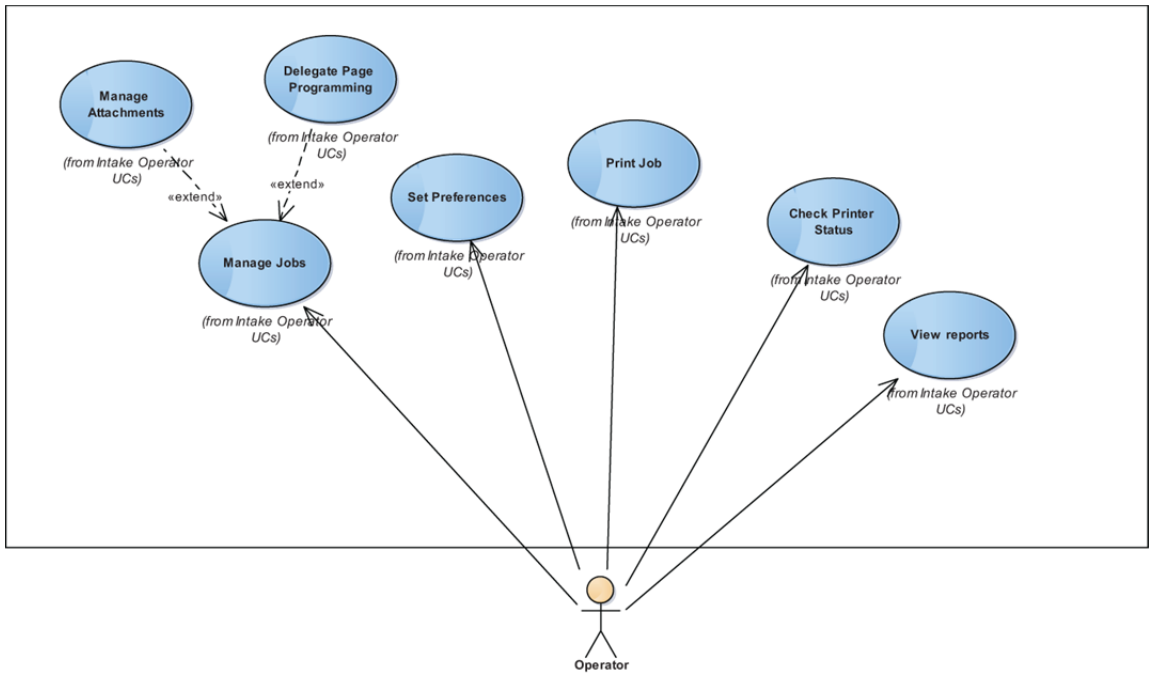
1.3.2 Order Managers



The Order Manager:

- Has to log in to the system;
- Can manage the orders, including: list the orders, select one or more orders, delete one or more orders, create an order;
- Can manage the jobs inside a selected order, including: list the jobs, select one or more jobs, delete one or more jobs, edit a job;
- Can manage the files of a selected job;
- Can page program a selected job;
- Can print one or more selected jobs and orders;
- Can check printer status;
- Can create a 1-job order from an email;
- Can export payment history;
- Can set preferences in the working environment;
- Can view reports.

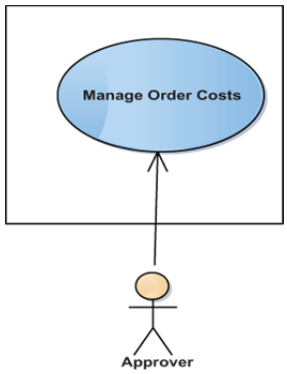
1.3.3 Operators



The Operator:

- Has to log in to the system;
- Can manage the jobs inside a selected order, including: list the jobs, select one or more jobs, delete one or more jobs, edit a job;
- Can manage the files of a selected job;
- Can page program a selected job;
- Can print one or more selected jobs and orders;
- Can check printer status;
- Can set preferences in the working environment;
- Can view reports.

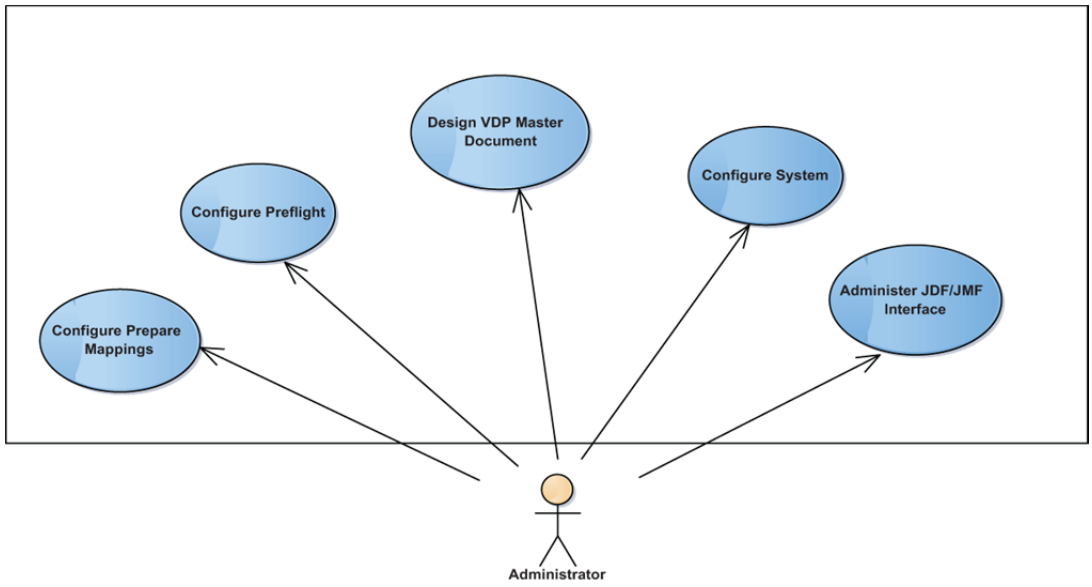
1.3.4 Approver



The Approver manages the cost approval requests. The Approver workflow starts when both Operator and Customer accept an order that is not yet paid. The following conditions are checked:

- Is the available budget of the cost center selected by the Customer exceeded?
- Is the spending limit per order for the Customer exceeded? The spending limit per order can be defined for the Customer, the default user group of the Customer, or the web shop.

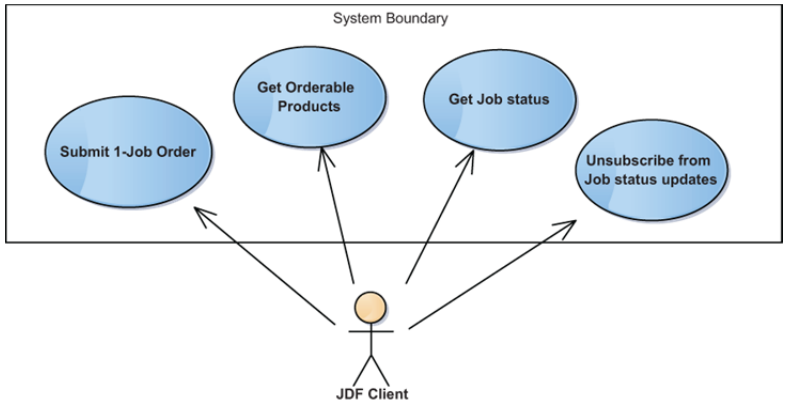
1.3.5 Administrator



The Administrator:

- Has to log in to the system;
- Can configure the system, including web shops and available product catalogs, mappings to PRISMAprepare, preflight, JDF/JMF interface;
- Can design VDP documents;
- Is a user with user role "Services".

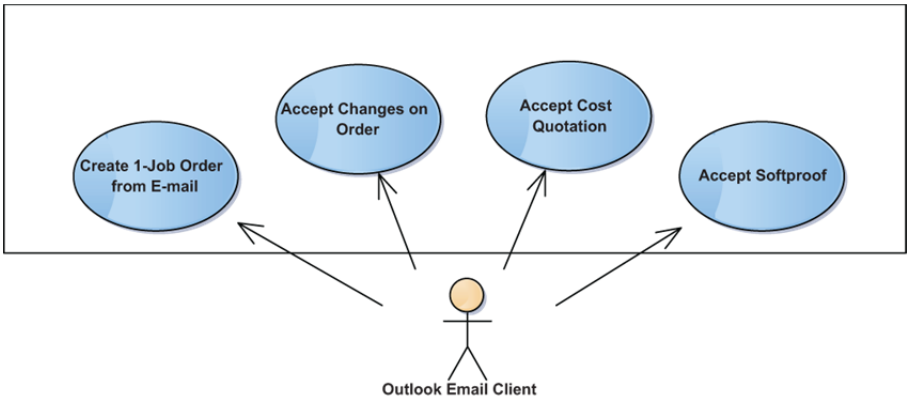
1.3.6 JDF Client



The JDF Client uses the JDF/JMF interface to interact with PRISMAdirect. The JDF Client:

- Can retrieve the job status;
- Can retrieve orderable products;
- Can unsubscribe from job status updates;
- Can submit a 1-job order, based on JDF ticket for a job.

1.3.7 Outlook Email Client



The Outlook Email Client uses the Outlook AddIn to interact with PRISMAdirect. The Outlook Email Client:

- Can create a 1-job order from an email;
- Receives emails about an order. Via the emails, it can:
    - Accept changes and resubmit an order
    - Accept quotation
    - Accept proof PDF

1.4 PRISMAdirect services and accounts

The default user that runs the PRISMAdirect services is:

- The currently logged on Windows user when the current computer is member of a domain. The currently logged on Windows user has local administrator rights.
- The “DocWorker” user when the current computer is not a member of a domain.

The IT policy of the customer can be that services must run without local administrator rights. During installation of PRISMAdirect, a custom user without local administrator rights can be created to run the PRISMAdirect services.

The user that runs the JDD service can be configured in the “Configuration” workspace. PRISMAdirect will automatically add all required access rights to that user account.

The following services are deployed on the PRISMAdirect server and/or web servers:

- **Print Automatic Processing Service**
  This service performs page counting, page preview generation, merge and native file conversion. It writes to log file “ProcessingService.log”.

- **Print Job Data Dispatcher**
  This service uploads files during job submission and dispatches actions on jobs in the system to the Print Automatic Processing Service. It writes to log file “JobDataDispatcher.log”.
- **Print Monitoring Service**
  This service handles notifications on changes (Orders/Files/Order status) from the JDF Framework and it caches data for the web client. It writes to the log files “MonitoringService.log”, the “MonitoringWCF.log” and “LicenseState.log”.
- **Print Import Service**
  This service imports orders from a local or remote file system, via hot folders. It writes to log file “ImportService.log”.
- **Print Export Service**
  This service exports orders into archive files, into the configured export folder. It writes to log file “ExportService.log”.
- **JDF Framework**
  This service handles user management and order storage on disk. It writes to log file “FW-OceJdfFramework-Trace.log”.
- **Print JDF Service**
  This service imports orders from JDF/JMF endpoints. It writes to log file “JdfService.log”.
- **Print Prepare Manager Service**
  This service performs the actions that involve PRISMA Core. For example, apply automation templates, VDP master/data source validation, etc. It writes to log file “PrepareManagerService.log”.
- **Print CleanUp Service**
  This service removes files that are no longer needed. It writes to log file “CleanUpService.log”.
- **Print Cost Manager Service**
  This service computes cost estimation, quotation and handles budget approval and operations on cost centers. It writes to the log files “CostManagerService.log” and “CostManagerWCF.log”.
- **Print License Monitoring Service**
  This service checks the license. It writes to log file “LicenseMonitoringService.log”.
- **Print Machine Manager**
  This service handles the IIS configuration. It writes to log file “MachineManagerService.log”.
- **Print ORS Service**
  This service handles the connection to Océ Remote Service. It writes to log file “ORSService.log”.
- **Print Synchronization Service**
  This service runs only on the remote component “Web server”. It handles the synchronization of settings between the server and the remote web server. It writes to log file “SynchronizationService.log”.
- **Print Uniflow Interface Service**
  This service handles the connection to uniFLOW. It writes to log file “UniflowInteropService.log”.
- **Print CSVLog Service**
  This service is always disabled.

The following service is deployed on client PCs:

- **Print Bootstrap Service**
  This service synchronizes the automation templates in PRISMAprepare with PRISMAdirect. It

writes to the log files “Bootstrap.log” for the web bootstrap executable and “BootstrapService.log” for the Print Bootstrap Service.

The following service is deployed on all computers where PRISMA Core is installed:

- **PRISMAprepare ORS service**
  This service handles the connection between PRISMAprepare and Océ Remote Service.

The following table shows which services run on each component of PRISMAdirect.

Server	Web server	Client PC
• Print Automatic Processing Service • Print Job Data Dispatcher • Print Monitoring Service • Print CleanUp Service • Print Cost Manager Service • Print License Monitoring Service • Print Machine Manager • Print ORS Service • Print Import Service • Print Export Service • JDF Framework • Print JDF Service • Print Prepare Manager Service • Print Uniflow Interface Service • Print CSVLog Service (disabled) • PRISMAprepare ORS service	• Print Automatic Processing Service • Print Job Data Dispatcher • Print Monitoring Service • Print CleanUp Service • Print Cost Manager Service • Print License Monitoring Service • Print Machine Manager • Print ORS Service • Print Synchronization Service (on remote web server only)	• Print Bootstrap Service • PRISMAprepare ORS service

1.5 Configurations of PRISMAdirect and its deployment

PRISMAdirect can be installed in a number of configurations on one or more computers. Each computer runs a server OS.

Configuration	Composition
Centralized on-premise	Server + Web Server installed on *one* computer
Extended on-premise	Server installed on *one* computer+ one or more Web Servers installed on separate computers
Centralized on-premise (w/o Web Shop)	Server installed on *one* computer

The server and the other components of PRISMAdirect can be installed on different computers. The different computers can be inside or outside the LAN where the server resides. When a web server is outside the LAN, it is called a remote web server.

Configuration	Composition
All computers in the LAN	Server + Web Server(s) + Client PCs in LAN
Only server in LAN	Server in LAN, Web Server(s) + Client PCs outside LAN
Server, Web Server + Client PCs in LAN, remote Web Server + Client PCs outside LAN	Server, Web Server(s) + Client PCs in LAN, remote Web Server(s) + Client PCs outside LAN

2 System security

2.1 Security assessment

A security assessment is performed on PRISMAdirect using Burp Suite Professional. The software is tested for compliance to:

- The internal technical standard used by Océ - A Canon Company.
- OWASP Top 10 Most Critical Web Application Security Risks (https://www.owasp.org/index.php/Top_10)
  No high severity problems are detected, see the “PRISMAdirect – security assessment” report.

2.2 Programming languages and technology

- The development language used for PRISMAdirect is C# 5.0 on .NET Framework 4.5.
- The Web UIs are built using HTML5, CSS and Javascript. The server side of the websites is built with C# on ASP.NET MVC. Other technologies used include jQueryUI, Knockout.js, SignalR and Bootstrap.

2.3 Antivirus software, proxy servers and web filter servers

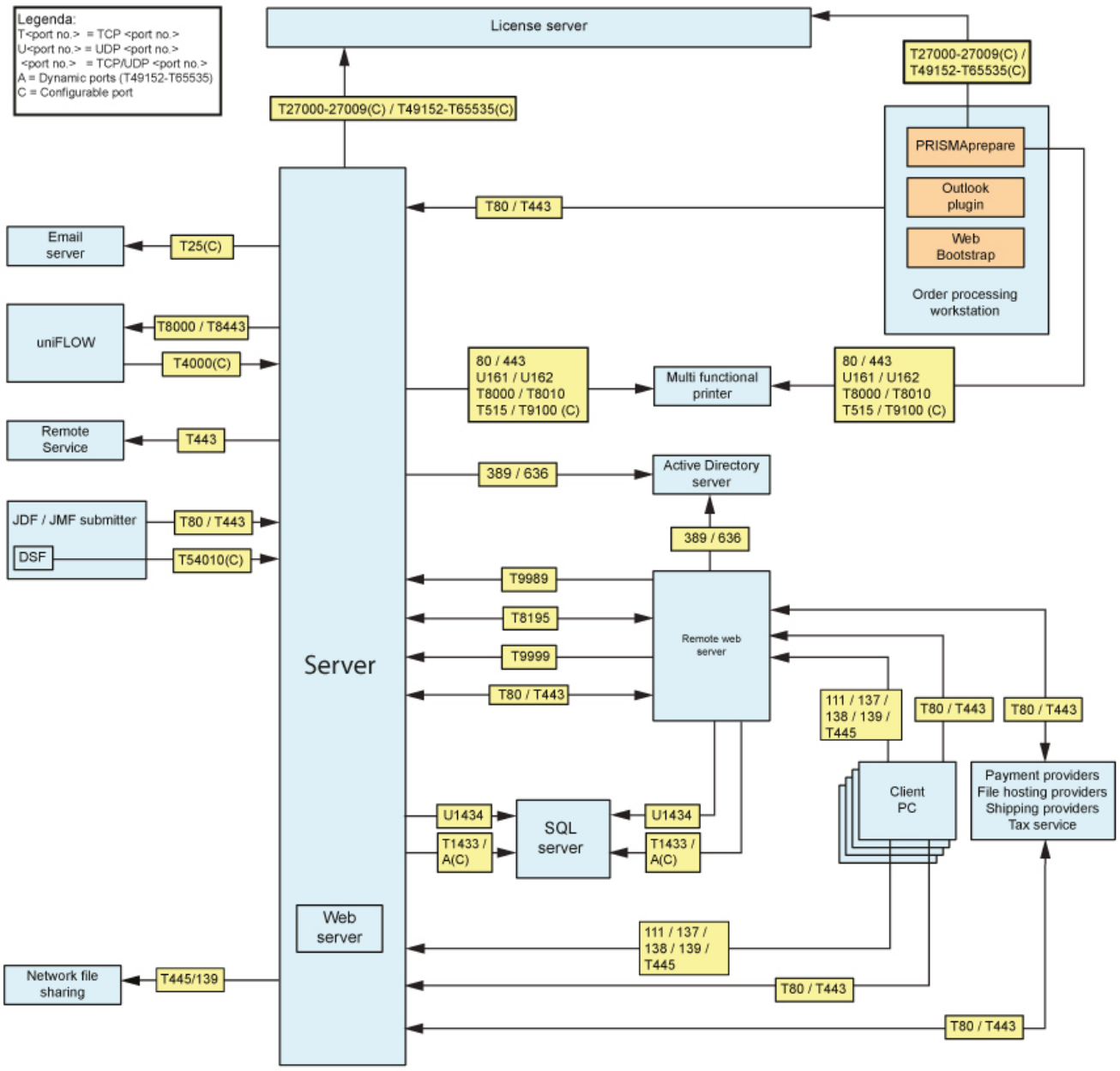
Antivirus software is encouraged as long as it does not lock legitimate files especially in temporary folders. The following temporary folders are used by PRISMAdirect and should be excluded from antivirus scanning:

- C: \Windows\TEMP\PRISMAdirect
  This is the default temporary folder path. The path can be changed in the “Configuration” workflow.
- C: \ProgramData\Oce\PRISMAprepare\Temp\

Proxy servers and web filter servers must not block or tamper with the traffic between clients and PRISMAdirect servers. Either create rules on these computers, or do not route the traffic to/from PRISMAdirect via these servers.

3 Network security

3.1 Diagram of the protocols and ports



The following tables list the protocols and port numbers used by PRISMAdirect.
Legenda for the tables:
(C) = configurable port

3.2 PRISMAdirect server

Component	Application protocol	Protocol & port no.	Direction	Main purpose
License server	Proprietary	TCP 27000 –27009 (C) TCP 49152 – 65535 (C)	Outbound	
License monitoring	Proprietary	TCP 9989	Inbound	Print License Monitoring Service used by server and remote web server
SQL Server instance	SQL	TCP 1433 TCP 49152 – 65535 (C)	Outbound	SQL Server default instance uses by default 1433. For Named instances, the TCP port is a dynamic port determined at the time the Database Engine starts, published via SQL Server Browser Service (broker). Each named instance uses a unique port.
SQL Server Browser Service	SQL	UDP 1434	Outbound	
Email server	SMTP	TCP 25 (C)	Outbound	
uniFLOW		TCP 8000 TCP 8443	Outbound	
uniFLOW		TCP 4000 (C)	Inbound	
Océ Remote Services	HTTPS	TCP 443	Outbound	
JDF/JMF submitter	HTTP HTTPS	TCP 80 TCP 443	Inbound	80 and 443 are the default ports. Check the port number in the reply message triggered by message “QueueStatus”.
JDF/JMF submitter - DSF		TCP 54010 (C)	Inbound	DSF is a special endpoint for a JDF / JMF submitter. Note: TCP 54010 (C) for PD 1.3 and higher. TCP 54001 (C) for PD 1.2.x and earlier.
Order processing workstation	HTTP HTTPS	TCP 80 TCP 443	Inbound	
Active Directory server	LDAP LDAPS	TCP/UDP 389 TCP/UDP 636	Outbound	(Secure) LDAP communication for user authentication and user profile.

				The exact user profile data that is retrieved is configurable.
JDF Framework user agent	JMF	TCP 8195	Inbound / outbound	Component used to make remote LDAP servers available on the PRISMAdirect server
Remote web server		TCP 9999	Inbound	Port used for signalR notifications
Remote web server	HTTP HTTPS	TCP 80 TCP 443	Inbound / outbound	
Network file sharing	SMB / CIFS	TCP 445 TCP 139	Outbound	TCP 445: SMB file sharing. The implementation of the SMB protocol is OS dependent. TCP 139: NetBIOS Session Service
Client PC	NetBIOS	TCP / UDP 111 UDP 137 UDP 138 TCP 139 TCP 445	Inbound	Web driver. The web driver uses the following five ports: 111: RPC 137: NetBIOS Name Service 138: NetBIOS Datagram Service 139: NetBIOS Session Service TCP 445: Printer sharing
Client PC	HTTP HTTPS	TCP 80 TCP 443	Inbound	
Payment providers	HTTP HTTPS	TCP 80 TCP 443	Inbound / outbound	Third party integration
File hosting services	HTTP HTTPS	TCP 80 TCP 443	Inbound / outbound	Third party integration
Tax services	HTTP HTTPS	TCP 80 TCP 443	Inbound / outbound	Third party integration
Shipping providers	HTTP HTTPS	TCP 80 TCP 443	Inbound / outbound	Third party integration
Multi-functional printer	HTTP HTTPS SNMP SNMP JMF JMF LPR/RAW	TCP / UDP 80 TCP / UDP 443 UDP 161 UDP 162 TCP 8000 TCP 8010 TCP 515 / T9100(C)	Outbound	HTTP(S): Data to printers SNMP 161 + SNMP 162: status JMF 8000: Canon controllers JMF 8010: EFI controllers LPR 515: Printer port RAW 9100 (C): Printer port
Internal ports	Proprietary	TCP 8732 TCP 54000 TCP 8098 TCP 8099 TCP 9988 TCP 54001		The services of PRISMAdirect use these ports for communication with the web hosted components of PRISMAdirect. TCP 8732: Print Uniflow Interface

				Service TCP 8098: Print Cost Manager Service TCP 8099: Print Monitoring Service TCP 9988: Print Job Data Dispatcher TCP 54000: Print Prepare Manager Service TCP 54001: opened internally on the loopback interface (127.0.0.1/localhost) by the Print Machine Manager service. For PD 1.2.x and earlier, TCP 54001 was also used externally for DSF JMF clients.

3.3 Remote web server

Component	Application protocol	Protocol & port no.	Direction	Main purpose
Active Directory server	LDAP LDAPS	TCP/UDP 389 TCP/UDP 636	Outbound	(Secure) LDAP communication for user authentication and user profile. The exact user profile data that is retrieved is configurable.
SQL Server instance	SQL	TCP 1433 TCP 49152 – 65535 (C)	Outbound	SQL Server default instance uses by default 1433. For Named instances, the TCP port is a dynamic port determined at the time the Database Engine starts, published via SQL Server Browser Service (broker). Each named instance uses a unique port.
SQL Server Browser Service	SQL	UDP 1434	Outbound	
License monitoring	Proprietary	TCP 9989	Outbound	Print License Monitoring Service
JDF Framework user agent	JMF	TCP 8195	Inbound / outbound	Component used to make remote LDAP servers available on the PRISMAdirect server
Server		TCP 9999	Outbound	Port used for signalR notifications
Server	HTTP HTTPS	TCP 80 TCP 443	Inbound / outbound	
Client PC		TCP / UDP 111	Inbound	Web driver. The web driver uses the

	NetBIOS	UDP 137 UDP 138 TCP 139 TCP 445		following five ports: 111: RPC 137: NetBIOS Name Service 138: NetBIOS Datagram Service 139: NetBIOS Session Service TCP 445: Printer sharing
Client PC	HTTP HTTPS	TCP 80 TCP 443	Inbound	
Payment providers	HTTP HTTPS	TCP 80 TCP 443	Inbound / outbound	Third party integration
File hosting services	HTTP HTTPS	TCP 80 TCP 443	Inbound / outbound	Third party integration
Tax services	HTTP HTTPS	TCP 80 TCP 443	Inbound / outbound	Third party integration
Shipping providers	HTTP HTTPS	TCP 80 TCP 443	Inbound / outbound	Third party integration
Internal ports		TCP 8098 TCP 8099 TCP 9988 TCP 54001		The services of PRISMAdirect use these ports for communication with the web hosted components of PRISMAdirect. TCP 8098: Print Cost Manager Service TCP 8099: Print Monitoring Service TCP 9988: Print Job Data Dispatcher TCP 54001: opened internally on the loopback interface (127.0.0.1/localhost) by the Print Machine Manager service. For PD 1.2.x and earlier, TCP 54001 was also used externally for DSF JMF clients.

3.4 License server

Component	Application protocol	Protocol & port no.	Direction	Main purpose
License server	Proprietary	TCP 27000 –27009 (C) TCP 49152 – 65535 (C)	Inbound	

3.5 Order processing workstation

Component	Application protocol	Protocol & port no.	Direction	Main purpose
License server	Proprietary	TCP 27000 –27009 (C) TCP 49152 – 65535 (C)	Outbound	License for PRISMAprepare
Server	HTTP HTTPS	TCP 80 TCP 443	Outbound	
Multi-functional printer	HTTP HTTPS SNMP SNMP JMF JMF LPR/RAW	TCP / UDP 80 TCP / UDP 443 UDP 161 UDP 162 TCP 8000 TCP 8010 TCP 515 / T9100(C)	Outbound	HTTP(S): Data to printers SNMP 161 + SNMP 162: status JMF 8000: Canon controllers JMF 8010: EFI controllers LPR 515: Printer port RAW 9100: Printer port

3.6 Client PC

Component	Application protocol	Protocol & port no.	Direction	Main purpose
Server & remote web server	NetBIOS	TCP / UDP 111 UDP 137 UDP 138 TCP 139 TCP 445	Outbound	Web driver. The web driver uses the following five ports: 111: RPC 137: NetBIOS Name Service 138: NetBIOS Datagram Service 139: NetBIOS Session Service TCP 445: Printer sharing
Server & remote web server	HTTP HTTPS	TCP 80 TCP 443	Outbound	

4 Access control

PRISMAdirect allows only authenticated users and computers to access sensitive information. PRISMAdirect restricts access to users with user accounts registered in PRISMAdirect or users registered in Active Directory.

The user role determines the access privileges of each user. For example, a user can be allowed access to only the “Order processing” workspace. Users can access the system at any time according to their access privileges. The roles are managed by the JDF Framework.

Passwords are stored in the SQL database using salted SHA-256 Hash. Salting renders existing rainbow tables useless, which are typically used for brute forcing hashing algorithms.

PRISMAdirect guards against malicious input to prevent the leakage of user authentication information and customer information. A number of techniques are implemented to avoid hacker attacks such as SQL injections* during communication through a web browser:

- The .NET API for sanitizing is used to verify input values
- The .NET form authentication feature is used
- The session ID is changed on every login

* SQL injection: Tamper Database or destroy, delete or acquire data by inserting SQL text in user input fields for Database access.

PRISMAdirect supports Single Sign-On using Windows Authentication with LDAP servers.

- User account data is sent (outbound) to the LDAP server when Windows Authentication is used. The following data is sent:

Function	Data	Windows Authentication	
		Information sent to Domain Server	Information retrieved from Domain Server
Windows Authentication	Domain	Yes	-
	User name	Yes	-
	Password	Yes	-

5 Data and data security

5.1 Data at rest

Generally, PRISMAdirect stores all received data indefinitely. PDF files and the complete tickets are stored on disk without encryption. Orders, jobs and files can be deleted by operators and order managers.

Access tokens of file hosting services and payment providers may be:
- Disposed directly after use or after a while.
- Stored on disk when option “Keep me logged on” for the concerning provider is enabled.

PRISMAdirect caches information from LDAP-servers for a maximum of one day. The information is refreshed:
- Each time the information is requested
- Each night

Sent emails are not stored, they are (re)generated when sending them.
License information from the license server is cached and periodically renewed.
No payment data whatsoever is stored on the PRISMAdirect system.

5.2 Data in transit

5.2.1 Web browser

PRISMAdirect and the web browser transmit data during a number of operations:
- Submit an order that contains one or more jobs with one or more files and tickets.
- Add files to existing jobs.
- Import an archive file to create an order. An archive file can contain files and tickets.
- Download the files of each job.

PRISMAdirect digitally signs all communication through web browsers. The used handshake protocol is the industry standard TLS.
Setting "IE Enhanced Security Configuration" must be disabled for Internet Explorer 11.

In addition to the regular website resources, the PRISMAdirect specific data sent over the network is presented in the following table:

Component	Application protocol	Protocol & port no.	Direction	Main purpose
Order processing workstation	HTTP HTTPS	TCP 80 TCP 443	Outbound	Job data, order data, system settings, action (e.g. create order), preview, data validation, status

Client PC	HTTP HTTPS	TCP 80 TCP 443	Outbound	Job data, system settings, action (e.g. create order), preview, data validation, status

Status notifications are implemented as SignalR notifications (http://signalr.net/). More information about data exchanged by SignalR components can be found in the official documentation: http://www.asp.net/signalr

Each browser communicates with the PRISMAdirect server via the web API for retrieving and sending all data. The data is JSON serialized when using the web API.

5.2.2 File hosting services

PRISMAdirect can retrieve files for new and existing jobs from file hosting services. The file hosting services are outside the LAN where the PRISMAdirect server resides.

The following data is exchanged with a file hosting service:

1. The user is authenticated to the file hosting service via a secure authentication method called OAuth (http://oauth.net/).
2. As a result of the OAuth process, the user receives an access token passed back to PRISMAdirect.
3. PRISMAdirect, using the access token:
   - Sends the desired container ID and receives the list of contents for that container using the storage API. Now, the user can browse the content of the file hosting service via PRISMAdirect.
   - The user selects all files to be downloaded. For each file, PRISMAdirect sends a file URI via the storage API. The requested files are downloaded and added to the job.

PRISMAdirect uses the following storage API methods:

- Oauth2/authorize
- Oauth2/token
- Auth/token/from_oauth1
- Files/get_metadata
- Files/download
- Files/list_folder
- Files/list_folder/continue
- Users/get_current_account

For a full description of Dropbox, see
https://www.dropbox.com/developers/documentation/http/documentation

Component	Application protocol	Protocol & port no.	Direction	Main purpose
File hosting	HTTP	TCP 80	Inbound /	PDF files, native files

provider	HTTPS	TCP 443	outbound	

5.2.3 Import service

PRISMAdirect can create orders directly from the file system using the import service:

- Import an archive file to create an order. An archive file can contain files and tickets.
- Import PDF files using a default ticket.
- The DPconvert module can convert Xerox RDO archive files into PDF files. The import service can import the PDF files.

Any folder supported by the Windows File System can be configured as an import folder for PRISMAdirect. Import folders can also be created on network shares.

The import service monitors the folder and automatically retrieves new files with the correct extensions for that folder. The accepted extensions depend on the configuration of the import folder:

- Normal orders: ZIP
- Legacy job: XML + referenced PDF file(s)
- JDF ticket orders: JDF + referenced PDF file(s)
- Scanned jobs: PDF
- 'PDF only' and 'Always accept orders and jobs': PDF, XLS, XLSX, XLSM, XLSB, XML, CSV, MDB, ACCDB, TXT, ZIP (depends on the chosen product type)

Component	Application protocol	Protocol & port no.	Direction	Main purpose
Network file sharing	SMB / CIFS	TCP 445 TCP 139	Outbound	TCP 445: SMB file sharing. The implementation of the SMB protocol is OS dependent. TCP 139: NetBIOS Session Service

5.2.4 Export service

PRISMAdirect can export orders to the file system using the export service.

Any folder supported by the Windows File System can be configured as an export folder for PRISMAdirect. Export folders can also be created on network shares.

The export service automatically exports all orders that match an export query. For each order, the export service generates an archive file of the order, its jobs, the files and the tickets. The archive file is then dropped into the export folder.

Component	Application protocol	Protocol & port no.	Direction	Main purpose
Network file sharing	SMB / CIFS	TCP 445 TCP 139	Outbound	TCP 445: SMB file sharing. The implementation of the SMB protocol is OS dependent.

				TCP 139: NetBIOS Session Service

5.2.5 Scan link

Scanned jobs can be received through the scan link. The scan link is an import folder configured as “Scanned jobs”. See 5.2.3 Import service.

5.2.6 Outlook AddIn

Customers can submit one or more files via Outlook. The operator can create an order from the files using the Outlook AddIn. PRISMAdirect imports the order from Outlook.

The Outlook AddIn allows the operator to create orders directly from Outlook. When creating a new order, the following data is sent to PRISMAdirect:

- Each file attached to the email.
- Metadata:
    - Email body,
    - UserID,
    - User email address
    - For each file: name: a generated GUID, a path on disk

When accepting an order, the following data is sent to PRISMAdirect:

- The order GUID. The order GUID is retrieved from the email subject
- An action timestamp
- An action signature using a private (shared) key to authenticate the operation

Component	Application protocol	Protocol & port no.	Direction to server	Main purpose
Client PC	HTTP HTTPS	TCP 80 TCP 443	Outbound	Includes data from Outlook AddIn

5.2.7 JDF compatible submitter using JDF/JMF endpoints

A JDF compatible submitter can submit:

- A PDF file and a JDF ticket to the import service. This is an optional submission method.
- A JDF ticket and one or more files to the server. This is the default submission method.
- Each change in the job status is sent to the JDF compatible submitter.

A JDF compatible submitter is any application that complies to the JDF standard.

The Job Definition Format (JDF) is a technical standard being developed by the CIP4 organization. The Job Messaging Format (JMF) is the language used to communicate between JDF agents and controllers. JMF is part of the JDF specification.
PRISMAdirect implements CIP4 JDF Specification 1.3, see:
https://confluence.cip4.org/download/attachments/7405591/CIP4%20JDF%20Specificataion%201.3.pdf?api=v2

PRISMAdirect supports the following JMF commands:
- SubmitQueueEntry (job submission)
- QueueStatus (including subscription)
- StopPersistentChannel (stop subscription)

PRISMAdirect supports the following JMF query:
- QueryKnownDevices (returns the products as defined in the “Product & order editor”)

PRISMAdirect adheres to JDF/JMF printing process standardization. It allows job submission from any 3rd party and provides job status feedback for JDF-enabled client applications.

PRISMAdirect supports the following submission types (inbound data):
- JMF message with link to JDF ticket
- MIME with link(s) to PDF files
- MIME that includes the PDF files

PRISMAdirect sends status feedback to JDF clients:
- On request
- Subscription-based, when status changes internally

Component	Application protocol	Protocol & port no.	Direction	Main purpose
JDF/JMF submitter	HTTP HTTPS	TCP 80 TCP 443	Inbound	Data, status 80 and 443 are the default ports. Check the port number in the reply message triggered by message “QueueStatus”.
JDF/JMF submitter - DSF		TCP 54010 (C)	Inbound	Data, status DSF is a special endpoint for a JDF / JMF submitter. Note: TCP 54001 (C) for PD 1.2.x and earlier. TCP 54010 (C) for PD 1.3 and higher.

5.2.8 Web Bootstrap

PRISMAdirect can open a number of external applications when you install the web bootstrap. The web bootstrap can download a file for editing and then upload it again into the system.
- The web bootstrap executable allows the operator to page program a PDF file using PRISMAprepare. The Web Bootstrap calls an API provided by PRISMA Core to open PRISMAprepare.
- The web bootstrap executable allows the operator to edit a PDF file in a PDF editor, e.g. Adobe Acrobat.
- The Print Bootstrap Service synchronizes the automation templates.

The operator can open a file to page program it. An XML file with extension “OED” is downloaded into the browser. The XML file with the “OED” extension is registered with the Web Bootstrap application. The XML file contains the metadata required for the Web Bootstrap:

- PRISMAdirect URLs to download and upload the file,
- Status updates,
- Order GUIDs, etc.

See 6.1 Web Bootstrap for detailed information concerning the contents of the XML file.

The Web Bootstrap and PRISMAdirect exchange data when the file is opened:

1. The file is downloaded (outbound) on the client to be page programmed.
2. PRISMAprepare is opened.
3. A notification is sent (inbound) to PRISMAdirect that the file is being page programmed.

The Web Bootstrap and PRISMAdirect exchange data after the file is page programmed:

1. The page programmed file is uploaded (inbound) back to PRISMAdirect.
2. Metadata in the XML file is sent to PRISMAdirect to identify the uploaded file. Additional information about the page programming is also sent: Printer name, print result, number of B&W pages and number of colour pages.
3. Job status is updated (inbound notification).

The Print Bootstrap Service sends the following data (inbound) to PRISMAdirect:

- When an automation template is created or edited, it is packed in a ZIP file and sent to the PRISMAdirect server
- When an automation template is deleted, a signal is sent to the PRISMAdirect server

The Print Bootstrap Service sends an action signature using a private (shared) key to authenticate the operations to the server.

Component	Application protocol	Protocol & port no.	Direction	Main purpose
Client PC	HTTP HTTPS	TCP 80 TCP 443	Outbound	PDF files, status, automation templates

5.2.9 LDAP server

PRISMAdirect can retrieve available user information from a LDAP server.

Multiple LDAP servers can be configured in PRISMAdirect. The following data is exchanged:

- User account data is sent (outbound) to the LDAP server when Windows Authentication is used:
  - Domain,
  - User name
  - Password
- User information is retrieved (inbound) from the LDAP server about users and user groups. Standard LDAP queries and traffic are generated when retrieving user information.

PRISMAdirect caches the user information. The information is refreshed:
- Each time the user information is requested
- Each night

The LDAP information described above can also be exchanged between the server and a web server via a proprietary protocol.

Component	Application protocol	Protocol & port no.	Direction	Main purpose
Active Directory server	LDAP LDAPS	TCP/UDP 389 TCP/UDP 636	Inbound	(Secure) LDAP communication for user authentication and user profile. The exact user profile data that is retrieved is configurable.

5.2.10 Email server

PRISMAdirect uses an email server to automatically send email messages on specific events. For each event, a specific email template is used.

PRISMAdirect sends specific email messages for a number of workflows, for example:
- Web user self-registration
- Cost approval workflow
- Various steps in the processing of jobs (accept, reject, finalize, etc.)
- Etc.

Component	Application protocol	Protocol & port no.	Direction	Main purpose
Email server	SMTP	TCP 25 (C)	Inbound	Data

5.2.11 PRISMAproduction

Optionally, PRISMAdirect can send jobs to PRISMAproduction using the printer driver of PRISMAproduction. The communication is one-way only. No status information is sent back from PRISMAproduction to PRISMAdirect.

5.2.12 Printers

PRISMAdirect can send page programmed and non-page programmed PDF files to the printers and receive status information. Also, PRISMAprepare can send page programmed PDF files directly to the printers.

PRISMAdirect can import the media catalogue from PRISMAsync controllers and EFI controllers.

PRISMAdirect handles print related tasks using the PRISMA Core component. This component:

- Manages printers and their configuration
- Handles print jobs

The PRISMA Core is responsible for printer communication.

A print protocol must be selected for standard TCP/IP printers with a printer driver. For each printer, the print protocol can be either LPR or RAW. LPR always uses TCP 515. The default port for RAW is TCP 9100, but this port is configurable. Add a rule to the firewall depending on the selected print protocol and port.

Component	Application protocol	Protocol & port no.	Direction	Main purpose
Multi-functional printer	HTTP HTTPS SNMP SNMP JMF JMF LPR/RAW	TCP / UDP 80 TCP / UDP 443 UDP 161 UDP 162 TCP 8000 TCP 8010 TCP 515 / T9100(C)	Outbound	HTTP(S): Data to printers SNMP 161 + SNMP 162: status JMF 8000: Canon controllers JMF 8010: EFI controllers LPR 515: Printer port RAW 9100: Printer port

5.2.13 Payment providers

PRISMAdirect sends and receives payment information to/from a number of payment providers. The payment providers are outside the LAN where the PRISMAdirect server resides.

The following scenario is an example of data that can be exchanged between PRISMAdirect and the payment provider. The actual communication depends on the selected payment provider.

During payment initialization:

1. PRISMAdirect sends initialization data to the payment provider that may include details like:
   - Provider specific settings to identify the merchant, etc.
   - Currency
   - Items, e.g.: Name, Quantity, Price
   - User data, e.g.: First name, Last name, Country, State, City, Address, ZIP code , Telephone number, Email
   - Callback URL(s) to be redirected back to PRISMAdirect
   - Notification URL(s) for post-payment
2. The payment provider sends a payment URL or token to PRISMAdirect.
3. The user is redirected to the payment website, pays and is redirected back to the PRISMAdirect web shop with a transaction response or a token.

During payment finalize (CAPTURE and/or acknowledge):

1. The payment provider sends a provider specific response with status, transaction details, etc to PRISMAdirect via a client or a CAPTURE response.
2. PRISMAdirect sends data required for the capture command to the payment service.
3. The payment provider may send transaction details to PRISMAdirect which may be stored until the transaction has finished.
   Transaction details that may be received and stored can be: transaction id, status, payer details, etc. The gateway can transmit some internal fields as part of the PRISMAdirect - gateway communication protocol. For example: tokens and signatures. This information may be temporarily stored as part of a persistence mechanism allowing a computer/service restart without losing the state of an ongoing transaction. See the documentation of the concerning provider for the used API methods.
4. PRISMAdirect may send a capture request to the payment provider. The capture request, if supported, contains provider specific parameters and transaction details.

When the operator refunds the customer, PRISMAdirect sends refund commands to the payment provider. During payment refund:

1. PRISMAdirect sends the transaction ID(s) and provider specific data to the payment provider.

During post payment notifications:

1. The payment provider sends specific data containing status, details, etc concerning changes of the transaction status to PRISMAdirect.

For the Paypal specific implementation, see https://developer.paypal.com/docs/classic/express-checkout/gs_expresscheckout/
PRISMAdirect uses the following API methods:

- SetExpressCheckout
- DoExpressCheckoutPayment
- GetExpressCheckoutDetails
- RefundTransaction

For the Worldpay specific implementation, see http://support.worldpay.com/support/kb/gg/corporate-gateway-guide/content/home.htm
PRISMAdirect uses the following API methods:

- Submit (XML hosted)
- Inquiry (XML manage)
- Modify (XML manage)

For the Ingenico specific implementation, see http://payment-services.ingenico.com/int/en/ogone/support/guides/integration%20guides/e-commerce and https://payment-services.ingenico.com/int/en/ogone/support/guides/integration%20guides/directlink
E-commerce integration is used during payment and no server to server communication is involved unless an automatic cancel or refund is required.
For cancel or refund, PRISMAdirect uses the following API methods:

- Maintenance request (DirectLink): DES and RFS operations

For the PayBox specific implementation, see http://www1.paybox.com/wp-content/uploads/2014/02/ManuelIntegrationPayboxSystem_V6.2_EN.pdf and http://www1.paybox.com/wp-content/uploads/2014/06/ManuelIntegrationPayboxDirect_V6.3_EN.pdf
Paybox integration is used during payment and no server to server communication is involved unless an automatic cancel or refund is required.
For cancel or refund, PRISMAdirect uses the following API methods:

- Paybox Direct or Paybox Direct Plus: Operation types 5 and 14

Component	Application protocol	Protocol & port no.	Direction	Main purpose
Payment provider	HTTP HTTPS	TCP 80 TCP 443	Inbound / outbound	Payment transaction, refund, transaction details, post-payment notification

5.2.14 Service provider for tax calculation

PRISMAdirect sends and receives tax information to/from a service provider for tax calculation. The service provider for tax calculation is outside the LAN where the PRISMAdirect server resides.

PRISMAdirect communicates with the service provider for tax calculation when:

- The tax is calculated for an order.
- The order is finalized.
- The order is canceled.

During the tax calculation:

1. PRISMAdirect caches the tax calculation requests. To optimize the API call frequency, PRISMAdirect uses a cached request to send the new tax data.
2. PRISMAdirect sends data to the service provider that include details like:
    a. Web shop origin address and the customer's address
    b. For each job: the product type and the estimated price.
3. The service provider for tax calculation sends:
    a. The tax values for each job
    b. If applicable, a corrected address if the provided address contains a recoverable errors. An error is returned if the provided addresses are not valid and recoverable.

When the order is finalized:

1. PRISMAdirect sends the same data as during the initial tax calculation.
2. The calculated tax is committed to the system of the service provider for tax calculation.

When the order is cancelled:

1. The calculated tax is cancelled by contacting the system of the service provider.

For the Avalara specific implementation, see https://developer.avalara.com/api-reference/avatax/rest/v1/methods/

PRISMAdirect uses the following API methods of Avalara:

- GetTax
- ValidateAddress
- CancelTax

Component	Application protocol	Protocol & port no.	Direction	Main purpose
Tax services	HTTP HTTPS	TCP 80 TCP 443	Inbound / outbound	Address validation and correction, Tax calculation

5.2.15 Shipping providers

PRISMAdirect sends and receives shipping information to/from a number of shipping providers. The shipping providers are outside the LAN where the PRISMAdirect server resides.

To request a quote:

1. PRISMAdirect sends the following data to one or more shipping providers:
   - Web shop origin address and the customer's address
   - An order can be shipped in one or more packages. For each package:
     - Type
     - Weight
     - Dimensions
     - Insurance fee
2. Depending on the shipping provider, the request is done for all service types in one API call or in multiple successive API calls.
3. The shipping provider responds with the shipping price for each package in combination with each service type.

To confirm the shipping request:

1. PRISMAdirect sends the same data as during the request of a quote.
2. For each package, the shipping provider returns:
   - Delivery date
   - Tracking number
   - Shipping label

For the DHL specific implementation, see https://xmlportal.dhl.com/

PRISMAdirect uses the following API operations:

- GetQuote (Rate Quote service)
- ShipmentRequest (Shipment Processing service)

For the FedEx specific implementation, see http://www.fedex.com/us/developer/

PRISMAdirect uses the following API operations:

- getRates (RateService)
- track (TrackService)
- validateShipment (ShipService)
- processShipment (ShipService)
- validatePostal (CountryService)

For the UPS specific implementation, see https://www.ups.com/upsdeveloperkit
PRISMAdirect uses the following API operations:

- AV (Address Validation API)
- Rate (Rating API)
- ShipConfirm (Shipping API)
- ShipAccept (Shipping API)

Component	Application protocol	Protocol & port no.	Direction	Main purpose
Shipping provider	HTTP HTTPS	TCP 80 TCP 443	Inbound / outbound	Shipping price calculation and request, tracking number and label

5.2.16 uniFLOW

PRISMAdirect can be integrated (paired) with uniFLOW. Before pairing, the required ports must be open, or forwarded when the servers are in different LANs. After pairing, PRISMAdirect passes a public key to the JDF Framework. The JDF Framework handles the user authentication on behalf of PRISMAdirect. The uniFLOW server behaves like an LDAP sever.

- A user with rights to the budget management workflow logs in to PRISMAdirect. PRISMAdirect sends the concerning authentication information to uniFLOW. uniFLOW sends available user information pertaining to the budget management workflow back to PRISMAdirect.
- PRISMAdirect can receive jobs from uniFLOW. A job consists of a uniFLOW job ticket and files.
- PRISMAdirect can update the cost centers managed by uniFLOW with budget information.
- PRISMAdirect can request accounting data from uniFLOW.
- PRISMAdirect can send accounting data to uniFLOW.

uniFLOW developed by NT-ware is one of the leading products in print, scan and device management, see (http://nt-ware.com/home/products/uniflow/about-uniflow.html). Together with PRISMAdirect, a proprietary protocol has been developed for integration. The following data categories are exchanged:

- Accounting
  PRISMAdirect collects accounting information. Periodically, uniFLOW initiates an extraction process to receive the accounting information from PRISMAdirect. PRISMAdirect sends the extraction response to uniFLOW. uniFLOW updates the accounting report.
- Budget management
  PRISMAdirect requests from uniFLOW:
  - Cost center list related to a specified user
  - Budget authorization for a specific cost center / user combination.
  - Budget update for a specific cost center / user combination.
- User management
  PRISMAdirect requests from uniFLOW:
  - User, user attributes, user authentication, user group membership.
  - Group, group members.

See 6.2 uniFLOW for the detailed data that is sent between PRISMAdirect and uniFLOW.

Communication to uniFLOW is signed to guard against tampering and replay attacks. The underlying protocol is RSA. The initial keys exchange for the asymmetric protocol RSA is done during a short time window under the user's supervision and acknowledgement.
All the messages are XML UTF-8 encoded. Each party has its own asymmetric key pair (public and private keys). Each party has knowledge of the public key of the other party.

Component	Application protocol	Protocol & port no.	Direction	Main purpose
uniFLOW		TCP 8000 TCP 8443	Inbound	
uniFLOW		TCP 4000 (C)	Outbound	

5.2.17 Océ Remote Service

PRISMAdirect sends a heartbeat to Océ Remote Service (ORS) to check the connection. Upon request by the administrator, ORS pushes license updates to PRISMAdirect.

Component	Application protocol	Protocol & port no.	Direction	Main purpose
Océ Remote Services	HTTPS	TCP 443	Inbound	

5.2.18 PRISMAprepare

The media catalogue of PRISMAprepare can be exported to a file. PRISMAdirect can import the media catalogue using this file.

For detailed information about data moving via the Web Bootstrap, see paragraph 5.2.8 Web Bootstrap.

5.2.19 Web driver

The web driver is a printer driver which can be installed via Point and Print on any client device.

1. The web driver generates and sends (inbound) the job GUID and PostScript file to PRISMAdirect. The web driver sends the PostScript file using:
   - Point and Print (version 3 drivers) for Microsoft OS
   - LPD printing for OS X

   Detailed information concerning the data exchange for the OS protocols can be found in the OS documentation.
2. The web driver opens the web browser on the client device. It sends the job GUID to PRISMAdirect to take over the submission process, i.e. the ticket configuration part. From this point on, the communication becomes regular web client communication

Component	Application	Protocol & port no.	Direction	Main purpose

	protocol			
Client PC	NetBIOS	TCP / UDP 111 UDP 137 UDP 138 TCP 139 TCP 445	Inbound	Web driver. The web driver uses the following five ports: 111: RPC 137: NetBIOS Name Service 138: NetBIOS Datagram Service 139: NetBIOS Session Service TCP 445: Printer sharing

5.2.20 Screen saver

A notification is sent to subscribers via SignalR when an order is created or changed. The screen saver is also subscribed to this notification channel.

Status notifications are implemented as SignalR notifications (http://signalr.net/). More information about data exchange by SignalR components can be found in the official documentation: http://www.asp.net/signalr

Component	Application protocol	Protocol & port no.	Direction	Main purpose
Client PC	HTTP HTTPS	TCP 80 TCP 443	Outbound	

5.2.21 License server

PRISMAdirect retrieves the license information from the remote license server via a proprietary protocol. The license information is cached on the server. Periodically, PRISMAdirect polls for any changes in the license information. The following license information is checked:

- Name
- Version
- Maximum instances
- Used instances
- Expiration date

Component	Application protocol	Protocol & port no.	Direction	Main purpose
License server	Proprietary	TCP 27000 –27009 (C) TCP 49152 – 65535 (C)	Inbound	

5.2.22 SQL server

PRISMAdirect uses a SQL server as a database engine. PRISMAdirect can install and use a new SQL server. PRISMAdirect can also connect to a SQL server already used by the customer.
The SQL server stores the following data:

- Job-related metadata
  A set of ticket fields - not the complete ticket - for performance and filtering reasons.
- PRISMAdirect configuration
- Cost centers configuration and status, approval workflow status
- Accounting data and related information
- Payment history

A TCP connection using its standard SQL communication protocol is used to exchange the data between PRISMAdirect and the SQL Server.
PRISMAdirect creates and uses the following databases:

1. ConfigStore
   Configuration storage of various settings (general configuration, user data, web shop settings, etc.). The tables used are:
   - Config_Attributs
   - Config_Category
   - Config_Object
   - Config_Refs
   - Search_Criteria
2. CostStore
   Storage of the cost centers structure, their current status (spent/reserved budgets) and tracking of approval workflow status for orders. The tables used are:
   - CostCenters
   - CostRejected
   - CostReserved
   - CostSpent
3. CustomJobQueues
   Light usage, tracking of job queues. The tables used are:
   - QueuesV4
4. DeviceInfoRepository
   This database is currently not used. It is present for historical and compatibility reasons. The available tables are:
   - DeviceAttributes
   - DeviceData
5. JobInfoRepository
   Storage of job-related metadata and internal details regarding job storage on the file system, links, etc. The tables used are:
   - DeviceQueues
   - JobAttributes
   - JobData
   - MultipleIndexes
   - NodeEntries
6. PrintAccounting
   Storage of all data that is accounting related. The data is grouped on various topics. The tables used are:

- __MigrationHistory
- FinishingAction
- ImageSettings
- JobCustomItems
- JobImageSettings
- JobItems
- JobMediaSettings
- MediaItem
- OrderCustomItems
- OrderItems
- TransactionInfoes (payment history)
- Transactions
- User

The information available in PRISMAdirect is always stored in the tables in the SQL server. When PRISMAdirect is integrated with uniFLOW, then the available information is both stored in the SQL server and sent to uniFLOW.

For the SQL server of the customer:

Component	Application protocol	Protocol & port no.	Direction	Main purpose
SQL Server instance	SQL	TCP 1433 TCP 49152 – 65535 (C)	Inbound	SQL Server default instance uses by default 1433. For Named instances, the TCP port is a dynamic port determined at the time the Database Engine starts, published via SQL Server Browser Service (broker). Each named instance uses a unique port.
SQL Server Browser Service	SQL	UDP 1434	Inbound	

6 Appendix

6.1 Web Bootstrap

The operator can open a file to page program it. An XML file with extension “OED” is downloaded into the browser. The XML file with the “OED” extension is registered with the Web Bootstrap application. The XML file with extension “OED” contains the following data:

Parameter	Observations
AttachmentKey	
AuthorizationToken	Token granting access to PRISMAdirect for future calls
BootstrapInstallerUrl	Link for download
FileDownloadAddress	Link for attachment download
FileName	Attachment name
FileUploadAddress	Link for prepared attachment upload
InstallationLanguage	Language of PRISMAdirect
JobQEntryID	Job GUID
Operation	Operation to perform
OperatorName	
SignalRConnectionID	
Version	Internal .oed version
Copies	Number of copies
DefaultPrinterName	If set in PRISMAdirect
DmAttributes (list of settings)	To pass to PRISMAprepare
JobName	
JobNumber	
PageProgrammCanceledUrl	Called without parameters when the operation is cancelled
PageProgrammCompletedUrl	Called without parameters when the operation is completed
PageProgrammErrorUrl	Called without parameters when an error is encountered
PageProgrammedStartedUrl	Called without parameters when the operation is started
XMLPrinterConfigs	Printer parameters

6.2 uniFLOW

The following data is exchanged via the uniFLOW interface:

User data

Field name	Description	Field type

First name	User's first name	String
Last name	User's last name	String
Login name	The login name of the user	String
Department	User's department	String
Location	User's location	String
Contact Address	Mailing address	String
Company	User's company name	String
Phone number	Phone number	String
Fax number	Fax number	String
Email address	Email address	String
Standard cost center	Default cost center of the user	String
Cost centers	List of cost centers that a user can use	List of strings

Group data

Field name	Description	Field type
Group name	The name of the group	String
Description	The description of the group	String
Standard cost center	The default cost center of the group	String
Cost centers	List of cost centers that can be used by the group	List of strings
User list	The list of users belonging to the group	List of strings

Cost center data

Field name	Description	Field type
Cost center name	The name of the cost center	String
Description	The description of the cost center	String
Access list	List of groups and users that can use the cost center	List of strings
Parent cost center name	Name of the parent cost center of this cost center	String
Expenses	Amount spent for this cost center (invariant format)	String
Spending limit	The spending limit for this cost center	String

Job data

Field name	Description	Field type
Job name	The name of the print job	String
Job ID	The ID of the job	String
Order	The order to which this job belongs to	String
Job comment	Additional comments added to the job	String
Product type	Type of product used for the job submission	String
User name	Name of the user that printed the job	String
Job info	• Reorder Y/N • Submission channel (driver/email) • Changes (What by who)	String

Job deadline date\time	Date and time of the job completion as requested by customer	String
Job completion date\time	Date and time of actual job completion by operator (marked it as ready)	String
Job completed by	User name of the operator that completed the job (marked it as ready)	String
Job dispatch date\time	Date and time of job dispatch to the customer	String
Job dispatched by	User name of the operator that dispatched the job	String
Job delivery date\time	Date and time of job delivery to the customer	String
Count	Number of pages in the print job. Zero for stationery products.	String
Copies	Number of copies of the print job or number of items for stationery products	String
Plexity	Indicates whether job should be printed simplex or duplex	String
Color	Indicates whether job should be printed in color or black & white	String
Covers	Indicates which covers should be present (none, front, back, both)	String
Cover media type	Indicates type of cover media	String
Cover media color	Indicates color of cover media	String
Cover media weight	Indicates weight of cover media	String
Document media size	Indicates size of document media	String
Document media type	Indicates type of document media	String
Document media color	Indicates color of document media	String
Document media weight	Indicates weight of document media	String
B/W pages	Number of black & white pages	String
Color pages	Number of color pages	String
Duplex pages	Number of duplex pages	String
Print pages	Number of printed pages (B/W & color, per size)	String
Scan pages	Number of scanned pages	String
Print area	Total print area of the print job	String
Standard price	Price calculated according to standard price profile	String
Price 1	Price calculated according to alternate price profile 1	String
Price 2	Price calculated according to alternate price profile 2	String
Price 3	Price calculated according to alternate price profile 3	String
Preparation duration	Time spent by the operator to prepare the job for printing	String
Printing duration	Time spent to print the job	String
Finishing duration	Time spent for finishing	String
Finishing	Type of finishing requested by customer	String
Finisher used	Name of the finisher used to finish the job	String
Printers used	Name of the printer used to print the job	List of strings
Labour	Cost of the manual actions performed on job	String
Final cost	Final cost of the print job charged to the customer	String

Order data

Field name	Description	Field type
Order name	The name of the order	String
Order ID	The ID of the order	String
User name	Name of the user that submitted the order	String
Order submission date\time	Date & time of order submission by the customer	String
Order accepted date\time	Date & time of order acceptance by the operator	String
Order accepted by	User name of the operator that accepted the order	String
Order quotation sent date\time	Date & time when order quotation was sent to the customer	String
Order quotation sent by	User name of the operator that sent the order quotation	String
Order quotation received date\time	Date & time of order quotation acceptance by the customer	String
Order quotation accepted by	Name of the person that accepted the job quotation (user or operator)	String
Order deadline date\time	Date and time of the order completion as requested by customer	String
Order completion date\time	Date and time of actual order completion by operator	String
Order completed by	User name of the operator that completed the order (marked it as ready)	String
Order dispatch date\time	Date and time of order dispatch to the customer	String
Order dispatched by	User name of the operator that completed the order	String
Order delivery date\time	Date and time of order delivery to the customer	String
Cost center	Cost center used to charge order	String
Final cost	Final cost of the print order	String
Jobs	List of jobs associated to the order	List of strings
Contact address	Address of contact for the order	String
Delivery address	Address of delivery for the order	String
Billing address	Address of billing for the order	String

Cost center transactions

Field name	Description	Field type
User name	Name of the user performing the transaction	String
Order ID	ID the order associated to the transaction (if applicable)	String
Transaction type	Type of transaction (regular purchase, reset expenses, modify spending limit)	String
Transaction value	Value added to expenses of cost center (0in case of reset) or new spending limit amount	String

Cost center	Cost center to which the transaction was billed	String