01.07.2019

Security Concept

1. Objective and Scope

The flexperto platform enables sales employees of large enterprises to engage with their customers online. As part of this User Experience, personal data both of your employees as well as your customers are processed by flexperto on your behalf. We classify part of this data as highly sensitive and private. The Objective of flexpertos IT-Security Policy is to ensure that bespoken data is treated and processed in a secure manner, in order to both protect end users privacy and your enterprise compliance to legal regulations. Therefore the following document describes rules and processes by which user and enterprise data processed by flexperto on behalf of enterprises are protected in regards to:

- **Confidentiality** - protection of data from unauthorized entities
- **Integrity** - ensuring the modification of data is handled in a specified and authorized manner
- **Availability** - a state of the flexperto platform and systems in which authorized users and personnel have continuous access to said data assets

Data processed within the flexperto platform are subject to the processes of Scheduling a Meeting, Video- & Audioconferencing, Screensharing, Whiteboard, Text chat, File Exchange, and contact data.

2. Stock Analysis

2.1 Rooms

Name	Type	Location	IT-Systems/Storage-Devices	Confidentiality	Integrity	Availability
R 1.01	Large Office	Neue Grünstraße 27 10179 Berlin	C01-C30 H01-H30	**Low** - While being the working place for flexperto employees, your enterprise and customer data are not processed on this location. Security of this location does not affect the security of service provided by flexperto to you	**Low** - While being the working place for flexperto employees, your enterprise and customer data are not processed on this location. Security of this location does not affect the security of service provided by flexperto to you	**Medium** - While being the working place for flexperto employees, your enterprise and customer data are not processed on this location. Security of this location does not affect the security of service provided by flexperto to you
R 1.02	Data-Center	Kleyerstrasse 79-89, 60326 Frankfurt am Main	M01-M11 P01-P10	High	High	High
R 1.03	Data-Center Staging and Failover	Versatel Solmsstr. Frankfurt am Main	M12-M22	Medium	Medium	Medium
R 1.04	Virtual Data-Center Amazon AWS Testing	Frankfurt	M23-M33	Low	Low	Low

2.2 Servers

The following Servers are Maintained by flexperto and part of the flexperto Platform. Legend:

- **ID** - for references on related pages or documents
- **Role** - The Role of the server in the platform

- **Domain / Ip** - The public domain / ip address of the server
- **Security Zone** - The security Zone of the server (refer to Firewalls)
- **Need of Confidentiality / Reason** - On a scale of "high", "medium", "low" the need of confidentiality (e.g. protection against unauthorized access to files and contents) of the server / The reason for this Assessment
- **Need of Integrity / Reason**- On a scale of "high", "medium", "low" the need of integrity (e.g. protection against deliberate or fraudulent manipulation of programs, manipulation of files) of the server / The reason for this Assessment
- **Need of Availability / Reasons**- On a scale of "high", "medium", "low" the need of availability (e.g. destruction, downtime, loss of data carriers) of the server / The reason for this Assessment

ID	Role	Domain	IP	ENVO	SEC-Zone	FW/IP	Data-Center	Need of Confidentiality / Reason	Need of Integrity / Reason	Need of Availability / Reasons
M01	Load Balancer	web01.live.flexperto.com	37.61.222.226	LIVE	10	ASA 5505 (37.61.222.254)	Velia.net Frankfurt	Low / The server does not store any data.	Low / The server does not store any data.	High / Impairment has a relevant impact on the availability of the services as perceived in total.
M02	Web-Application Server	app01.live.flexperto.com	37.61.222.231	LIVE	50	ASA 5505 (37.61.222.254)	Velia.net Frankfurt	High / The server stores documents and files uploaded by users which include personal data and might include Business Secrets.	High / Impairment has a relevant impact on the availability of the services as perceived in total.	High / Impairment has a relevant impact on the availability of the services as perceived in total.
M03	Contract Signature	insign01.live.flexperto.com	37.61.222.228	LIVE	50	ASA 5505 (37.61.222.254)	Velia.net Frankfurt	High / The server stores documents and files uploaded by users which include personal data and might include Business Secrets.	Medium / Impairment has only impact on the availability of parts of the services as perceived in total.	Medium / Impairment has only impact on the availability of parts of the services as perceived in total.
M04	WebSocket - Application Server	wss01.live.flexperto.com	37.61.222.230	LIVE	50	ASA 5505 (37.61.222.254)	Velia.net Frankfurt	High / The server stores documents and files uploaded by users which include personal data and might include Business Secrets.	Medium / Impairment has only impact on the availability of parts of the services as perceived in total.	Medium / Impairment has only impact on the availability of parts of the services as perceived in total.

M05	Monitoring	monitor01.live.flexperto.com	37.61.222.234	LIVE	50	ASA 5505 (37.61.222.254)	Velia.net Frankfurt	Low / The server does not store any data.	Low / Impairment has no impact on the availability of the services as perceived in total.	Low / Impairment has no impact on the availability of the services as perceived in total.
M06	Mail	mail01.live.flexperto.com	37.61.222.229	LIVE	50	ASA 5505 (37.61.222.254)	Velia.net Frankfurt	Medium / The server might store personal data (outbound emails) up to 10 minutes.	Medium / Impairment has only impact on the availability of parts of the services as perceived in total.	Medium / Impairment has only impact on the availability of parts of the services as perceived in total.
M07	Backup	backup01.live.flexperto.com	37.61.222.236	LIVE	100	ASA 5505 (37.61.222.254)	Velia.net Frankfurt	High / The server stores documents and files uploaded by users which include personal data and might include Business Secrets.	Medium / Impairment has only impact on the availability of the services in case of a disaster.	Medium / Impairment has only impact on the availability of the services in case of a disaster.
M08	Database Master	db02.live.flexperto.com	37.61.222.233	LIVE	100	ASA 5505 (37.61.222.254)	Velia.net Frankfurt	High / The server stores documents and files uploaded by users which include personal data and might include Business Secrets.	High / Impairment has a relevant impact on the availability of the services as perceived in total.	High / Impairment has a relevant impact on the availability of the services as perceived in total.
M09	Database Slave	db03.live.flexperto.com	37.61.222.228	LIVE	100	ASA 5505 (37.61.222.254)	Velia.net Frankfurt	High / The server stores documents and files uploaded by users which include personal data and might include Business Secrets.	Medium / Impairment has a relevant impact on the availability of the services as perceived in total.	Medium / Impairment has a relevant impact on the availability of the services as perceived in total in case of failure of M09
M10	Logging	logging01.live.flexperto.com	37.61.222.232	LIVE	100	ASA 5505 (37.61.222.254)	Velia.net Frankfurt	High / The server stores system internal service messages. Exposure can harm the bussiness of flexperto and security relevant data.	Low / Impairment has no impact on the availability of the services as perceived in total.	Low / Impairment has no impact on the availability of the services as perceived in total.

M11	Load Balancer	web01.staging.flexperto.com	146.0.229.167	Staging	10	ASA 5505 (146.0.229.162)	Velia.net Frankfurt	Low / The server does not store any data.	Low / The server does not store any data.	Medium / Impairment has a relevant impact on the availability of the services as perceived in total only in case of disaster.
M12	Web-Application Server	app01.staging.flexperto.com	146.0.229.168	Staging	50	ASA 5505 (146.0.229.162)	Velia.net Frankfurt	Medium / The server does not store documents and files uploaded by users but serves as a recovered fail over system in the case of disaster recovery.	Medium / Impairment has a relevant impact on the availability of the services as perceived in total. In case of disaster recovery it does.	Medium / Impairment has a relevant impact on the availability of the services as perceived in total. In case of disaster recovery it does.
M13	Contract Signature	insign01.staging.flexperto.com	146.0.229.169	Staging	50	ASA 5505 (146.0.229.162)	Velia.net Frankfurt	Medium / The server stores documents and files uploaded by users which include personal data and might include Business Secrets in the case of disaster.	Low / Impairment has only impact on the availability of parts of the services as perceived in total in the case of disaster.	Low / Impairment has only impact on the availability of parts of the services as perceived in total in the case of disaster.
M14	WebSocket - Application Server	wss01.staging.flexperto.com	146.0.229.172	Staging	50	ASA 5505 (146.0.229.162)	Velia.net Frankfurt	Medium / The server stores documents and files uploaded by users which include personal data and might include Business Secrets in the case of disaster.	Low / Impairment has only impact on the availability of parts of the services as perceived in total in the case of disaster.	Low / Impairment has only impact on the availability of parts of the services as perceived in total in the case of disaster.
M15	Monitoring	monitor01.staging.flexperto.com	146.0.229.173	Staging	50	ASA 5505 (146.0.229.162)	Velia.net Frankfurt	Low / The server does not store any data.	Low / Impairment has no impact on the availability of the services as perceived in total.	Low / Impairment has no impact on the availability of the services as perceived in total.

M16	Mail	mail01.staging.flexperto.com	146.0.229.170	Staging	50	ASA 5505 (146.0.229.162)	Velia.net Frankfurt	Low / The server might store personal data (outbound emails) up to 10 minutes in the case of disaster.	Low / Impairment has only impact on the availability of parts of the services as perceived in total in the case of disaster.	Low / Impairment has only impact on the availability of parts of the services as perceived in total in the case of disaster.
M17	Backup	backup01.staging.flexperto.com	146.0.229.163	Staging	100	ASA 5505 (146.0.229.162)	Velia.net Frankfurt	Medium / The server stores documents and files uploaded by users which include personal data and might include Business Secrets in case of a disaster.	Low / Impairment has only impact on the availability of the services in case of a disaster.	Low / Impairment has only impact on the availability of the services in case of a disaster.
M18	Database Master	db01.staging.flexperto.com	146.0.229.164	Staging	100	ASA 5505 (146.0.229.162)	Velia.net Frankfurt	Medium / The server stores documents and files uploaded by users which include personal data and might include Business Secrets in case of a disaster.	Medium / Impairment has a relevant impact on the availability of the services as perceived in total in case of a disaster.	Medium / Impairment has a relevant impact on the availability of the services as perceived in total in case of a disaster.
M19	Database Slave	db02.staging.flexperto.com	146.0.229.165	Staging	100	ASA 5505 (146.0.229.162)	Velia.net Frankfurt	Medium / The server stores documents and files uploaded by users which include personal data and might include Business Secrets in case of a disaster.	Medium / Impairment has a relevant impact on the availability of the services as perceived in total in case of a disaster.	Medium / Impairment has a relevant impact on the availability of the services as perceived in total in case of a disaster.
M20	Logging	logging01.staging.flexperto.com	146.0.229.166	Staging	100	ASA 5505 (146.0.229.162)	Velia.net Frankfurt	High / The server stores system internal service messages. Exposure can harm the bussiness of flexperto and security relevant data.	Low / Impairment has no impact on the availability of the services as perceived in total.	Low / Impairment has no impact on the availability of the services as perceived in total.

M21	Load Balancer	web01.test.flexperto.com	dynamic	Test	10		AWS Frankfurt	Low / The server does not store documents and files uploaded by users and only includes test data.	Low / The server does not store documents and files uploaded by users and only includes test data.	Low / The server does not store documents and files uploaded by users and only includes test data.
M22	Web-Application Server	app01.test.flexperto.com	dynamic	Test	50		AWS Frankfurt	Low / The server does not store documents and files uploaded by users and only includes test data.	Low / Impairment has no impact on the availability of the services as perceived in total.	Low / Impairment has no impact on the availability of the services as perceived in total.
M23	Contract Signature	insign01.test.flexperto.com	dynamic	Test	50		AWS Frankfurt	Low / The server does not store documents and files uploaded by users and only includes test data.	Low / Impairment has no impact on the availability of the services as perceived in total.	Low / Impairment has no impact on the availability of the services as perceived in total.
M24	Mail	mail01.test.flexperto.com	dynamic	Test	50		AWS Frankfurt	Low / The server does not store documents and files uploaded by users and only includes test data.	Low / Impairment has no impact on the availability of the services as perceived in total.	Low / Impairment has no impact on the availability of the services as perceived in total.
M25	WebSocket - Application Server	wss01.test.flexperto.com	dynamic	Test	50		AWS Frankfurt	Low / The server does not store documents and files uploaded by users and only includes test data.	Low / Impairment has no impact on the availability of the services as perceived in total.	Low / Impairment has no impact on the availability of the services as perceived in total.
M26	Monitor	monitor01.test.flexperto.com	dynamic	Test	50		AWS Frankfurt	Low / The server does not store documents and files uploaded by users and only includes test data.	Low / Impairment has no impact on the availability of the services as perceived in total.	Low / Impairment has no impact on the availability of the services as perceived in total.

M27	Backup	backup01.test.flexperto.com	dynamic	Test	100		AWS Frankfurt	Low / The server does not store documents and files uploaded by users and only includes test data.	Low / Impairment has no impact on the availability of the services as perceived in total.	Low / Impairment has no impact on the availability of the services as perceived in total.
M28	Database Master	db01.test.flexperto.com	dynamic	Test	100		AWS Frankfurt	Low / The server does not store documents and files uploaded by users and only includes test data.	Low / Impairment has no impact on the availability of the services as perceived in total.	Low / Impairment has no impact on the availability of the services as perceived in total.
M29	Database Slave	db02.test.flexperto.com	dynamic	Test	100		AWS Frankfurt	Low / The server does not store documents and files uploaded by users and only includes test data.	Low / Impairment has no impact on the availability of the services as perceived in total.	Low / Impairment has no impact on the availability of the services as perceived in total.
M30	Logging	logging01.test.flexperto.com	dynamic	Test	100		AWS Frankfurt	Low / The server does not store documents and files uploaded by users and only includes test data.	Low / Impairment has no impact on the availability of the services as perceived in total.	Low / Impairment has no impact on the availability of the services as perceived in total.

2.3 Clients

The following Clients are maintained by flexperto. Legend:

- **ID** - (H for mobile device / C for DesktopDevice) for references on related pages or documents
- **Name** - The Product Name of the client
- **Need of Confidentiality / Reason** - On a scale of "high", "medium", "low" the need of confidentiality (e.g. protection against unauthorized access to files and contents) of the server / The reason for this Assessment
- **Need of Integrity / Reason**- On a scale of "high", "medium", "low" the need of integrity (e.g. protection against deliberate or fraudulent manipulation of programs, manipulation of files) of the server / The reason for this Assessment
- **Need of Availability / Reasons**- On a scale of "high", "medium", "low" the need of availability (e.g. destruction, downtime, loss of data carriers) of the server / The reason for this Assessment

ID	Name	Need of Confidentiality / Reason	Need of Integrity / Reason	Need of Availability / Reasons
C01 - Cn	Desktop Clients (Win 10 Pro / OSX Sierra)	High / Sensitive data processed on behalf of customers is not being stored on devices. Access to services and servers only happens encrpyted (SSL/TLS/SSH) and through firewalls	High / Sensitive data processed on behalf of customers is not being stored on devices. Access to services and servers only happens encrpyted (SSL/TLS/SSH) and through firewalls	Low / Impairment can be bridged by additional devices.
H01 - Hn	Smartphones (Android & iOS)	High / Data processed on behalf of customers is not stored on the client itself. It is forbidden for employees to access administrative areas via smartphones. The possibility of misuse can not be technically eliminated.	High / Data processed on behalf of customers is not stored on the client itself. It is forbidden for employees to access administrative areas via smartphones. The possibility of misuse can not be technically eliminated.	Low / Performing administrative tasks via mobile clients is forbidden to coworkers

2.4 Services

The following Services are Maintained by flexperto. Legend:

- **ID** - for references on related pages or documents
- **MID** - The Service ID that provides this service
- **Name** - The Name of the service
- **Tech** - Technology of the service
- **Purpose** - The purpose of the service in the system
- **Personal Data** - The service provides or persists data that is personal
- **Need of Confidentiality / Reason** - On a scale of "high", "medium", "low" the need of confidentiality (e.g. protection against unauthorized access to files and contents) of the service / The reason for this Assessment
- **Need of Integrity / Reason**- On a scale of "high", "medium", "low" the need of integrity (e.g. protection against deliberate or fraudulent manipulation of programs, manipulation of files) of the service / The reason for this Assessment
- **Need of Availability / Reasons**- On a scale of "high", "medium", "low" the need of availability (e.g. destruction, downtime, loss of data carriers) of the service / The reason for this Assessment

ID	MID	Name	Tech	Purpose	Personal Data	Need of Confidentiality / Reason	Need of Integrity / Reason	Need of Availability / Reasons
S01		RDMBS	MySQL (Master)	Persistent Relational Data	Yes	**High** / Exposure of client data to unauthorized third parties can cause considerable damage to both flexperto and the customer.	**High** / Corrupted Data can cause depending services to be partially unavailable. Exposure to Users is possible.	**High** / Without access to this data store contractual duties towards customers can not be fulfilled. The service is therefore redundantly replicated

S02		RDMBS	MySQL (Slave)	Persistent Relational Data	Yes	**High** / Exposure of client data to unauthorized third parties can cause considerable damage to both flexperto and the customer.	**High** / Corrupted Data can cause depending services to be partially unavailable. Exposure to Users is possible.	**High** / Without access to this data store contractual duties towards customers can not be fulfilled. The service is therefore redundantly replicated
S03		EFK	ElasticSearch, Kibana, FluentD	LogFile Aggregation, Visualization and Analysis	Yes	**High** / Exposure of client data to unauthorized third parties can cause considerable damage to both flexperto and the customer.	**Low** / Corrupted Data has no impact on the delivery of the service in total.	**Low** / Corrupted Data has no impact on the delivery of the service in total.
S04		BACKUP	Bacula	Persistent Backup Management	Yes	**High** / Exposure of client data to unauthorized third parties can cause considerable damage to both flexperto and the customer.	**High** / Corrupted Data can render services as unavailable in the case of a recovery.	**High** / Systems can not be recovered when needed without this service. Thats why this service is hosted in a different site then the service that are to be backed up.
S05		MONITOR	Icinga2	Service and System Health and Availability Monitoring	No	**Medium** / Exposure of system data to unauthorized third parties can cause considerable damage to flexperto and degrade the overall security level of the platform.	**Low** / Corrupted Data has no impact on the delivery of the service in total.	**Medium** / Without this Service the availability of other services is not centrally visible. Their state and health has to be monitored manually in this case.
S06		LWS	Nginx/PHP	Core Web Service	Yes	**Medium** / The service itself does not store personal data but it exposes personal data. However Application Layer authentication and authorization ensure that data is only exposed according to the Rights & Permissions model. Exposure of system data to unauthorized third parties can cause considerably damage to flexperto and degrade the overall security level of the platform.	**Medium** / The service itself is stateless and the code base is version controlled. Integrity of the service itself ensured. However corrupted data served by underlying services can have an impact on the services availability.	**High** / Impairment has a relevant impact on the availability of the services as perceived in total.
S07		FS	RAID1/ext4	Document and File Storage	Yes	**High** / Exposure of client data to unauthorized third parties can cause considerable damage to both flexperto and the customer.	**High** / Corrupted Data can cause depending services to be partially unavailable. Exposure to Users is possible.	**Medium** / Impairment has an impact on the availability of parts of the services as perceived in total.
S08		HERMES	Nginx/NodeJS	PubSub/TextChat	Potentially	**High** / Data exchange can be personal data. Exposure of data exchanged to unauthorized third parties can cause considerable damage to both flexperto and the customer.	**Medium** / Corrupted Data has an impact on the availability of parts of the services as perceived in total.	**Medium** / Impairment has an impact on the availability of parts of the services as perceived in total.

S09		SIGNALING	Nginx/NodeJS	Signaling	No	**Low** / The service does not provide personal data.	**Medium** / Corrupted Data has an impact on the availability of parts of the services as perceived in total.	**Medium** / Impairment has an impact on the availability of parts of the services as perceived in total.
S10		WHITEBOARD	Nginx/NodeJS	Whiteboard	Potentially	**High** / Exposure of data exchanged to unauthorized third parties can cause considerable damage to both flexperto and the customer. Exchange of personal data over the whiteboard is considered an exception.	**Medium** / Corrupted Data has an impact on the availability of parts of the services as perceived in total.	**Medium** / Impairment has an impact on the availability of parts of the services as perceived in total.
S12		INSIGN	Tomcat/Java	Digital Signature	Yes	**High** / Exposure of client data to unauthorized third parties can cause considerable damage to both flexperto and the customer.	**Medium** / Corrupted Data has an impact on the availability of parts of the services as perceived in total.	**Medium** / Impairment has an impact on the availability of parts of the services as perceived in total.
S13		LOADBALANCING	HaProxy	LoadBalancing	No	**Low** / The service does not provide personal data.	**Low** / The service itself is stateless and the code base is version controlled. Integrity of the service itself ensured. The service does not depend on data stores.	**High** / Impairment has an impact on the availability of the complete services as perceived in total.

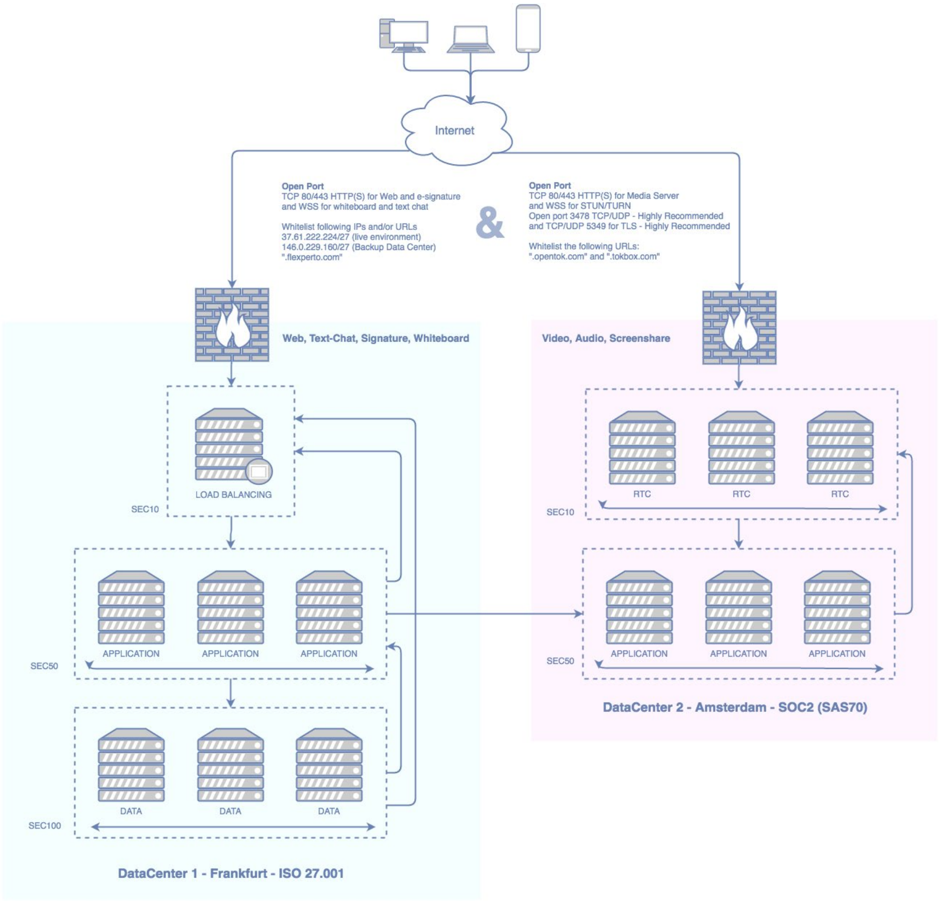
3. Glossary

Name	Description
User	A User as a natural person using one of the available services of the flexperto platform
Expert	An Expert is an authenticated natural person that offers services to customers on the flexperto platform
Customer	An Customer is an authenticated natural person that consumes services provided by experts on the flexperto platform
Administrator	An Administrator is an authenticated natural person that has access to any data, regardless of ownership and permission.
Flexperto-Administrator	A Flexperto-Administrator is an employee of flexperto with administrator privileges to access the live and staging platform technical and functional configuration.
Flexperto-Developer	A Flexperto-Developer is an employee of flexperto with administrator privileges to access the development and testing platform technical and functional configuration.
Identity	The permission scheme of flexperto is identity-based. This means that a User can only be either an expert, or a customer or an administration. If he wants to use the platform as multiple identities, he has to create an account for each of the identities.
Meeting	A Meeting is the concept and data about 2 participants communicating with each other using one of flexpertos real time communication services (either spontaneously or agreed upon in advance)
Screensharing	Screensharing is one of flexpertos real time communication services, which allows a meeting participant to broadcast either his full screen or one of his desktop application windows to his counterpart
Whiteboard	The Whiteboard is one of flexpertos real time communication services, which allows a meeting participant to share documents, images and drawings with a counterpart as well as the capability to do basic collaboration on the shared contents.

eMail	eMail is one of flexpertos asynchronous communication services, which allows transmissions of notification messages from platform to user
Messages	Messages is one of flexpertos asynchronous communication services, which allows transmissions of messages between customers and experts
Chat	Chat is one of flexpertos real-time communication services, which allows transmissions of chat-messages between customers and experts

4. Network

The flexperto Network Infrastructure is developed with a focus on security and reliability. Next, to processes that guarantee harmonic and consistent operations, this includes proven Soft- and Hardware security Measurements:


Internet
Open Port
TCP 80/443 HTTP(S) for Web and e-signature
and WSS for whiteboard and text chat
Whitelist following IPs and/or URLs
37.61.222.224/27 (live environment)
146.0.229.160/27 (Backup Data Center)
".flexperto.com"
&
Open Port
TCP 80/443 HTTP(S) for Media Server
and WSS for STUN/TURN
Open port 3478 TCP/UDP - Highly Recommended
and TCP/UDP 5349 for TLS - Highly Recommended
Whitelist the following URLs:
".opentok.com" and ".tokbox.com"
Web, Text-Chat, Signature, Whiteboard
Video, Audio, Screenshare
LOAD BALANCING
SEC10
RTC
RTC
RTC
SEC10
APPLICATION
APPLICATION
APPLICATION
SEC50
APPLICATION
APPLICATION
APPLICATION
SEC50
DataCenter 2 - Amsterdam - SOC2 (SAS70)
DATA
DATA
DATA
SEC100
DataCenter 1 - Frankfurt - ISO 27.001

5. Firewalls

The flexperto infrastructure is secured towards intrusion and malicious interaction on multiple levels. This includes:

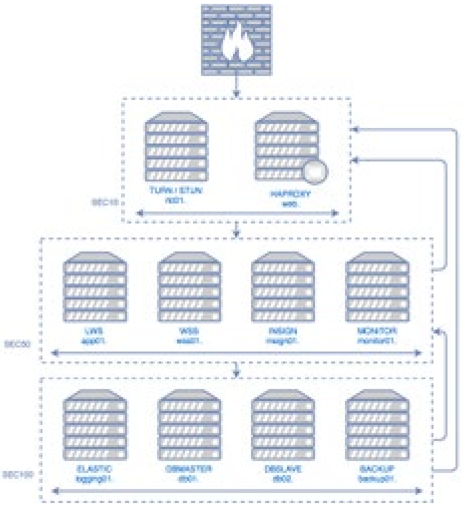
- A hardware firewall that every external request has to pass

- Software firewalls that ensure communication can only happen in well-defined directions
- WAF (Web Application Firewall) that protects against malicious Request Payload against OWASP Signatures

In addition, the flexperto infrastructure is layered into 3 Trust Zones:

- sec10 - (as known as DMZ (DeMilitarized Zone) Load Balancing / Web
- sec50 - Application Services
- sec100 - Persistent Data Services

Machines within a zone only accept traffic from the next less trustworthy zone. Direct access of services in zone sec50 and sec100 from external are prohibited by hard and software firewalls. All machines are equipped with an additional high secure (with an additional security component, known as "Switch Port in Private Mode") backup interface that allows operations without an impact on the network performance.



Firewall Rules

Communication between nodes in the flexperto network is secured using soft- and hardware firewalls. The following rules are applied:

ZONE	Port	Description
VPN => 10 / VPN => 50 / VPN => 100	22	Administrative and operational SSH access secured fia VPN
VPN => 10 / VPN => 50 / VPN => 100	ICMP	Network-Interface Availability checks on the ICMP Protocol
50 => 10 / 50 => 100	5666	Operating System Health Checks using the NRPE protocoll

VPN => 10	9911	LoadBalancer Statistics and Health Status (secured via VPN access)
* => 10	443	End-User facing HTTPS traffic
* => 10	80	End-User facing HTTP traffic (HSTS redirects to HTTPS)
10 => 50 / 50	4789, 7946	Virtual Network and Container Scheduler Clustering
50 => 100	3306	Relational Database Management System
50 => 100	27017, 27018, 27019	Document Database Management System
10 => 50 / 100 => 50	111, 24007, 24008, 49152	Shared clustered file system
50 => 100	9200	Log Aggregation Management System

6. Antivirus

The duty of antivirus detection and protection within flexperto realm resides with the application servers in the sec50 zone. Two software solutions are used here:

phpMussel is an antivirus detection software that analyzes request payload for trojans, viruses, malware and other threads based on ClamAV signatures and others. The payload is being analyzed and in case of a detected threat the request is being intercepted by the application server before any application code is being executed.

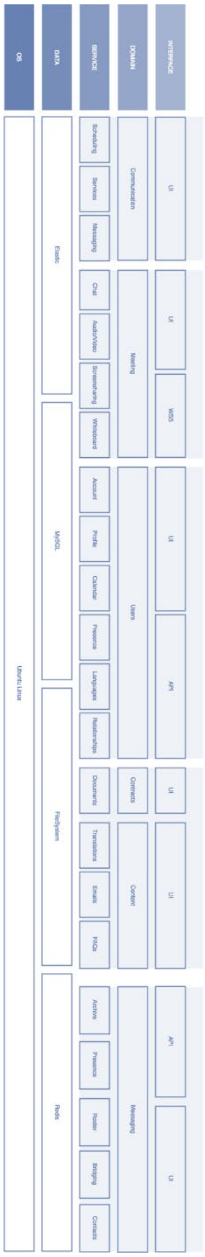
ClamAV is an antivirus detection software that analyzes request payload for trojans, viruses, malware and other threads based on ClamAV signatures and others. In contrast to phpMussel, ClamAV is used to scan the file system after requests have been processed. If a thread is identified, it is moved to a quarantine zone. This zone is excluded from backups and the incident is being logged. Incidents are regularly reviewed and the quarantine is cleared.

7. Platform Architecture

The Architecture of the flexperto Platform is structured into the following Layers:

- **Interface** - Used to expose the Business Logic to Users or foreign systems either as a User Interface, an API or a WebSocket
- **Domain** - Used to rather as a Business Layer then a technical Layer to cluster the Platform into groups relevant to provide meaningful Business-Logic and Business-Rule sets
- **Services** - Used as the technical component that provides Business-Logic to Interfaces

- **Data** - Used as storage and persistence facilities
- **OS** - Used as the Linux foundation on which services and data stores are running



8. Data Classification Scheme

The flexperto eService platform is designed as a multi-tenancy, service-oriented System. This means that a classic data classification approach is not valid anymore, since data may reside in one spot, but is processed and presented in multiple contexts within the System. That's why conceptually Data is grouped into Data-Bags within flexperto System, where the same data may reappear in several Data-Bags but has a different purpose and meaning within the Business-Context it is processed in. A DataBag consists of:

- **ID** - The id of the Data-Bag for revering on different pages/documents
- **Name** - A name of the Data-Bag
- **Description** - What the Data-Bag contains
- **Persistence Services** - If the data is made persistent, the IDs of the Services that handle persistence
- **Processing Services** - If the data is being processed, the IDs of the Services that handle processing
- **Presentational Services** - If the data is being presented, the IDs of the Services that handle the presentation
- **Persistence Location** - The location of the services that persist the data
- **Processing Location** - The location of the services that process the data
- **Presentation Location** - The location of the services that present the data

All documentation reflects the "per tenant architecture" which means: All persistent data per tenant is stored in an individual and logically separated data store.

ID	Name	Description	Persistence Services	Processing Services	Presentational Services	Persistence Location	Processing Location
DB01	Relational User data	All relational user data, such as account information, availability, communication history etc. are stored in the RDBMS Service and processed into the presentational service for user or system consumption by the LWS Service.	S01, S02, S04	S06	S06, S13	Germany	Germany
DB02	File Transfer	Files shared between users through file attachment to asynchronous messaging, meetings or Text-Chat	S07, S04	S06	S06, S13	Germany	Germany
DB03	Real-Time Messaging	Any real-time text messages shared within a session	S01, S02, S04	S08	S06, S08, S13	Germany	Germany
DB04	Whiteboard Documents	Documents uploaded and worked on within the whiteboard	S10	S10	S10, S13	Germany	Germany
DB05	Digital Signature data	Any contracts signed via the digital signature process and any biometric signature data stored within the contracts	S07	S12, S06	S12, S06, S13	Germany	Germany
DB06	RTC-Media in flight	All video/voice/screen-sharing data shared between users during a session which is routed via the RTC service platform		S11	S11, S06	Not stored	Germany

DB07	RTC-Media at rest	Any recordings of sessions. Recordings are encrypted, are stored only temporarily within the RTC service platform. The storage policy is for recordings to only be kept for the minimum time practical inside the RTC service platform to successfully deliver the output file to the service S07	S11 (temporarily), S07, S04	S11, S06	S06	Germany	Germany
DB08	RTC Metrics	Any data generated by the flexperto RTC service platform which is logged expressly for the purposes of operating the platform, understanding issues and improving performance. Such data includes: • API Traffic Logs • Control/Messaging Traffic • Media Server Logs • Analytics/Instrumentation Data • Platform Access Logs • IP-Adress	S11	S11	S11	USA, Germany	USA, Germany
DB09	Platform Activity Metrics	Any data generated by the flexperto CORE platform which is logged expressly for the purposes of operating the platform, understanding issues and improving performance. Such data includes: • Web Access Logs • Service Logs • Business Process Monitoring ○ The Action that was taken ○ The identity that performed the action ○ The success of the action ○ In case of failure action input/output	S03	S03	S03	Germany	Germany

DB01 Relational User data

While using flexperto, Users interact with the System and with each other. This data has to be made persistent, in order to provide a service that allows showing past messages for example. Personal Data being gathered and stored is of the following nature:

- **User and Account Data** - such as first name, last name but also presence and relationships
- **Calendars and CalendarEvents** - such as Event-Start and Event-End
- **Text-Chat History** - Message content as well as metadata such as delivery data and sender/receiver
- **Asynchronous Message History** - Message content as well as metadata such as delivery data and sender/receiver
- **Contract Meta-Data** - such as state (pending / signed) and signature date.

- **Uploaded Files Meta-Data** - such as MIME-type and original filename
- **Meeting Meta-Data** - such as participants and state (pending / confirmed / ongoing / canceled)

Encryption Policy: Using a firewalled 3-Tier Architecture, this data is never exposed directly to users. Data is always processed by the application Tier and therefore protected by authentication, authorization and In/Output-Validation and filtering measurements. On the flight, the data is inside as well as outside the DMZ always encrypted using SSL/TLS and one of these ciphers:

- ECDHE_RSA_WITH_AES_256_GCM_SHA384
- ECDHE_RSA_WITH_AES_128_GCM_SHA256
- ECDHE_RSA_WITH_AES_256_CBC_SHA384
- ECDHE_RSA_WITH_AES_256_CBC_SHA256

Private keys are used for global encryption, tenants do not have an individual private key.

At rest the underlying filesystem is encrypted using this cipher:

- AES-XTS-PLAIN64:SHA256

In addition, the Database System is encrypted using this ciphers:

- AES_256_CBC
- AES_256_ECB

Persistence Policy: Data is stored permanently and, in order to ensure maximum service integrity, only erased upon service discontinuation on a per tenant basis.

DB02 File Transfer

Within the flexperto platform, Users can exchange files by uploading them to the platform and providing access to other authenticated users in multiple places:

- **Text-Chat related files** - files that are exchanged within a Text-Chat
- **Contracts** - documents to be, or already signed
- **Profile Pictures** - profile pictures of experts that are publicly available even to guests / unauthenticated users
- **Message related files** - files that are attached to the asynchronous messaging /mail system
- **Meeting files** - files attached to meeting upfront or after the meeting occurred.

Encryption Policy: Using a firewalled 3-Tier Architecture, this data is never exposed directly to users. Data is always processed by the application Tier and therefore protected by authentication, authorization and In/Output-Validation and filtering measurements. On the flight, the data is inside as well as outside the DMZ always encrypted using SSL/TLS and one of these ciphers:

- ECDHE_RSA_WITH_AES_256_GCM_SHA384
- ECDHE_RSA_WITH_AES_128_GCM_SHA256
- ECDHE_RSA_WITH_AES_256_CBC_SHA384
- ECDHE_RSA_WITH_AES_256_CBC_SHA256

Private keys are used for global encryption, tenants do not have an individual private key.

At rest the underlying filesystem is encrypted using this cipher:

- AES-XTS-PLAIN64:SHA256

Persistence Policy: Data is stored permanently and, in order to ensure maximum service integrity, only erased upon service discontinuation on a per tenant basis.

DB03 Real Time Messaging

Within the flexperto platform, Users can exchange messages when entering a meeting room and within a meeting room via the text-chat. While being persisted in DB01 for later retrieval, this data-bag is concerned about the transmission of the message to the receiver in real time. A message includes personal data such as their content, referrals to possible file attachments as well as identifiers for sender and receiver.

Encryption Policy: This Data-Bag is transmitted from Client to Tier-1 LoadBalancer => Tier-2 Management Proxy => Tier-2 Application => Tier-2 Management Proxy => Tier-1 LoadBalancer => Client. This data flow utilizes a custom, proprietary protocol over secure WebSockets (WSS) along persistent connections between any web/mobile client and the flexperto platform. These connections between the client and server are only persisted for the lifetime of a session. On the flight, the data is inside as well as outside the DMZ always encrypted using SSL/TLS and one of these ciphers:

- ECDHE_RSA_WITH_AES_256_GCM_SHA384
- ECDHE_RSA_WITH_AES_128_GCM_SHA256
- ECDHE_RSA_WITH_AES_256_CBC_SHA384
- ECDHE_RSA_WITH_AES_256_CBC_SHA256

Private keys are used for global encryption, tenants do not have an individual private key.

At rest the underlying filesystem is encrypted using this cipher:

- AES-XTS-PLAIN64:SHA256

In addition, the Database System is encrypted using this ciphers:

- AES_256_CBC
- AES_256_ECB

Persistence Policy: Data is stored permanently and, in order to ensure maximum service integrity, only erased upon service discontinuation on a per tenant basis.

DB04 Whiteboard Documents

Within a meeting on the flexperto platform, Users can utilize the whiteboard to upload and present documents to each other. Users can add new text content as well as basic shapes and drawings to the documents and download the content of the whiteboard in the PDF-Format. The Whiteboard-Data as well as up- and downloaded documents are temporary persisted next to the service. While potentially personal data can be uploaded to the Whiteboard, this is typically not the use case.

Encryption Policy: This Data-Bag is transmitted from Client to Tier-1 LoadBalancer => Tier-2 Management Proxy => Tier-2 Application => Tier-2 Management Proxy => Tier-1 LoadBalancer => Client. This data flow utilizes a custom, proprietary protocol over secure WebSockets (WSS) along persistent connections between any web/mobile client and the flexperto platform. These connections between the client and server are only persisted for the lifetime of a session. On the flight, the data is inside as well as outside the DMZ always encrypted using SSL/TLS and one of these ciphers:

- ECDHE_RSA_WITH_AES_256_GCM_SHA384
- ECDHE_RSA_WITH_AES_128_GCM_SHA256
- ECDHE_RSA_WITH_AES_256_CBC_SHA384
- ECDHE_RSA_WITH_AES_256_CBC_SHA256

Private keys are used for global encryption, tenants do not have an individual private key.

At rest the underlying filesystem is encrypted using this cipher:

- AES-XTS-PLAIN64:SHA256

Persistence Policy: While Data is stored in order to ensure maximum service integrity during usage, the data is not accessible outside the service / distributed to other services. Data is deleted on resource demand basis.

DB05 Digital Signature data

Within a meeting on the flexperto platform, Users can utilize the digital signature service to upload contracts and sign them using touch-enabled devices. The user creates highly personal, potentially biometric data when signing a contract. This data is embedded into resulting documents only and not persisted anywhere else. This data bag is not persisting and only kept during the lifetime of a signature session. Resulting PDFs are encrypted and stored within DB02.

Encryption Policy: On the flight, the data is inside as well as outside the DMZ always encrypted using SSL/TLS and one of these ciphers:

- ECDHE_RSA_WITH_AES_256_GCM_SHA384
- ECDHE_RSA_WITH_AES_128_GCM_SHA256
- ECDHE_RSA_WITH_AES_256_CBC_SHA384
- ECDHE_RSA_WITH_AES_256_CBC_SHA256

Private Keys generated with the RSA algorithm and 2048bit length. In addition, content delivery within this data-bag is encrypted using the same Ciphers and based on HTTPS. Biometric data is embedded within the resulting PDF and encrypted via Private/Public Key, The private key lies with a notary in Germany.

Private keys are used for global encryption, tenants do not have an individual private key.

At rest the underlying filesystem is encrypted using this cipher:

- AES-XTS-PLAIN64:SHA256

Persistence Policy: While Data is stored in order to ensure maximum service integrity during usage, the data is not accessible outside the service / distributed to other services. Data is regularly deleted upon session recycling.

Service Partner

flexperto provides the digital signature Service in cooperation with the partner Intelligent Solution Services AG

DB06 RTC-Media in flight

Media Traffic: Media traffic is the audio/video/screen-sharing and related traffic that flows either in between clients directly (peer-peer) or via our platform between clients (routed, relayed mode). Media traffic is encrypted (using DTLS encrypted using AES_128_CM and 1024 bit keys) using secure RTP (sRTP) between clients and client/server and is subject to the following treatments:

Over the course of a media session, data is transferred between user endpoints in the following way:

- Pure Peer-to-Peer Mode: Media traffic is encrypted and sent between the clients directly with no contact with the RTC service. End to end encryption is achieved under this method.
- Relayed Mode: In cases where clients are behind NATs/Restrictive firewalls, encrypted media data is relayed between clients through TURN servers in the RTC service. End to end encryption is achieved under this method.
- Routed Mode: Routed sessions are explicitly routed through Media Servers in the RTC service. This is the mode required to perform:

1.
    1. Multi-party sessions
    2. Large-scale broadcast optimizations
    3. Intelligent quality control features and network adaptation
    4. Recording of any individual stream or the composed entire stream

Private keys are used for global encryption, tenants do not have an individual private key.

Media streams are decrypted in this mode while in the RTC Service environment and then encrypted prior to being routed to the Client browser/application. To maintain the real-time communication experience, decrypted packets of data are only processed via RAM for a fraction of a second prior to re-encryption. Decrypted data packets are never written to disk in standard video mode. Optional recording functions are outlined in section "Recording"

Intelligent Quality Control

The RTC platform features a series of advanced proprietary tools into its platform to maximize the quality of service and user experience in times of fluctuations in end-user network conditions. Some are automatically applied and others customizable for a customer’s specific use case. Examples of these tools include:

- Scalable multiparty: optimizing video quality on a per subscriber basis to maximize overall quality experienced in larger groups
- Audio Fallback: automatically switch to an audio-only mode in poor network conditions
- Adaptable framerate controls: ability to customize framerates based on network conditions to maximize quality and experience
- Audio Detection: user experience optimization by implementing responsive technology and layout control based on who is speaking in session.

The RTC Service is provided by TokBox. inc. The data center is located in Amsterdam

DB07 RTC-Media at rest

Session Recordings: Customers have the option of recording some/all of the sessions. flexperto does not record sessions by default and will only initiate recordings when explicitly instructed by a user of the platform in a session, given the administrator has given the user the appropriate rights to do so.

From an information security perspective, the two key pieces of information customers should know upfront are:

- Recordings are encrypted
- The recordings are stored for the minimum time possible within the RTC service and subsequently delivered to a long-term storage location in the flexperto platform. It is possible to send the recording to a storage location of the Customers choice.

Private keys are used for global encryption, tenants do not have an individual private key.

Encryption of recordings

flexperto recognizes that the content of a session is highly confidential information and therefore uses the following method of real-time encryption: Video streams are encrypted prior to being written to the disk of the server performing the recording. This encryption is performed as packets of data are added to the overall file and not at the conclusion of the recording. Encryption algorithms used are AES-256 CBC for the media and RSA-2048 key exchange (to encrypt the AES key).

Storage considerations

As described above, the RTC service requirement for recording storage is limited to being incidental to performing the function reliably and not intended to be a permanent source or hosting or storage. Once the recording is complete, the RTC Service will attempt to transfer any file via https to the Service S07.

- If the first attempt is successful, the RTC service will immediately delete the recording.
- If an error occurs, the RTC service will continue to attempt to deliver the recording for up to 2 hours by making up to 10 transfer attempts.
- Following any successful retry, deletion occurs immediately and if all attempts fail, the deletion will take place after the 2 hour retry period.

The RTC Service is provided by TokBox. inc. The data center is located in Amsterdam

DB08 RTC Metrics

The following section further details operation metrics and outlines the storage policy of the RTC Metrics data.

- API Traffic: These are secured HTTPS API calls (using 2048 bit keys and AES_128_CBC), which are invoked by server-side, and/or client-side services.

- Control/Messaging Traffic (Signalling): This messaging/control traffic data that utilizes a custom, proprietary protocol over secure WebSockets (WSS) (using 2048 bit keys and AES_128_CBC) along persistent connections between any web/mobile client and the flexperto RTC service platform. These connections between the client and server are only persisted for the lifetime of a session. Messaging/control traffic can be categorized in 2 ways:

  1. System Messages: include information about sessions, connections and media streams such as where a session is hosted, how many connections are in a session, stream bitrates, packet loss and whether a stream has audio or video or is being recorded.
  2. Client Callflow / Signalling: The RTC service supports sending messages between Clients (for example: when a User turns of his camera). This data is passed through the RTC service platform. The content of the messages is an encrypted point to point and is logged by flexperto and not logged or stored by TokBox Inc.

Storage policy and rationale

As outlined above flexperto is contracting TokBox Inc. as the technology provider for the RTC service. In order to provide best in class service, TokBox Inc. as a service provider is storing the following items as follows:

Potentially identifiable metrics – 30 days - IP Addresses:

- The RTC service collects IP addresses in raw format for a limited period of time in order to complement debugging and video quality analysis efforts (both at the individual session level and overall platform health) by both TokBox and flexperto's development team.
- Source IP address may not be available/logged if NAT (Network Address Translation) or PAT (Port Address Translation) is used by an End User or its ISP.
- flexperto also recognizes that IP addresses may, in some scenarios, be considered personally identifiable information, especially since this has consequences regarding the European Data Protection Law and for most Customers the German Data Protection Law. Customers should be aware that this IP address is collected in isolation from all other user-level data stored in the flexperto platform (which is not accessible by TokBox).
- Given that the information is a core component of efficient customer service, the access to the information is given to all customer-facing and engineering functions.
- Following 30 days, the raw format IP address is de-identified by way of an irreversible hashing function.

Non-identifiable metrics - Up to 3 years

- API Traffic: TokBox maintains logs from its API server components for the express purpose of analyzing and improving operational health.

- Control/Messaging Traffic: TokBox maintains logs from the Messaging server components for the express purpose of analyzing and improving operational health.
- Media Server Logs: Logs generated from media servers include items such as call quality metrics (packet loss, bitrates) stream state (added, removed, archived etc.), number of subscribers.
- Analytics/Instrumentation Data: Clients can essentially use HTTPS API calls to log instrumentation and quality of service, which is anonymized and aggregated in the analytics infrastructure.
- Platform access log entries will be maintained, containing the date and time the operation performed (connect, publish, etc.).

Private keys are used for global encryption, tenants do not have an individual private key.

At rest the underlying filesystem is encrypted using this cipher:

- AES-XTS-PLAIN64:SHA256

DB09 Platform Activity Metrics

Usage of the flexperto platform triggers multiple, system internal events which are logged in order to analyze operation metrics and therefore service integrity, security, and stability. The following Data is logged in this Data-Bag:

- Web Access Logs - including data such as IP-Address of the request origin, URL of the request and meta-data about the request
- Service Logs - including System-Health notifications and event trails/audits on service / OS-Level
- Business Process Monitoring - events that enable monitoring the state and health of business process monitoring. This includes per event:
    - The action that was taken
    - The identity that performed the action
    - The success of the action
    - In case of failure action input/output

Private keys are used for global encryption, tenants do not have an individual private key.

At rest the underlying filesystem is encrypted using this cipher:

- AES-XTS-PLAIN64:SHA256

Storage policy and rationale

Platform Activity Metrics are kept in order to ensure service integrity, security, and stability.

9. Application Security

Across the complete System, the following application level security features are in place:

- SSL: flexperto encrypts bidirectional web session traffic between the Services, Servers, and Clients

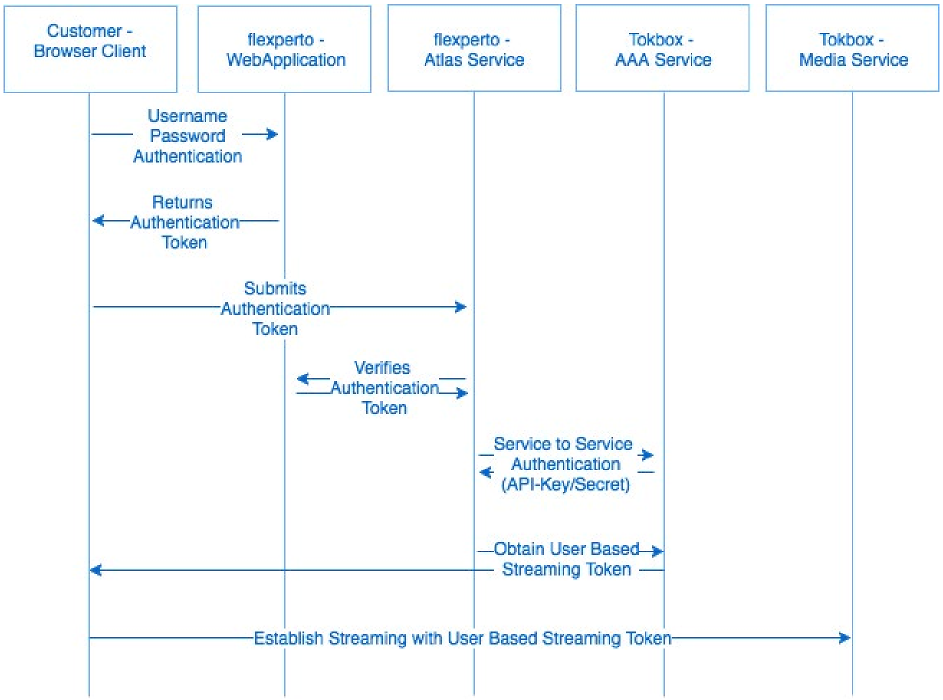
- HTTP Authentication: The flexperto RTC service uses industry-standard security technologies such as HTTPS support, secure RTP, HTTP authentication.
- Inter-Service Authentication / Authorization: Within the flexperto platform services authenticate and authorize against each as well as users approaching, using Tokens based on RFC 7591. Tokens are generated using HMAC256 of relevant API secret and associated with metadata.
- Secure WebSockets: There are two WebSocket connection modes: unencrypted (ws://) and encrypted (wss://). The flexperto service platform uses the encrypted WebSocket mode, using TLS/SSL encryption to encrypt all data sent to and from the server (including the initial handshake and response). This is the same encryption mechanism used for HTTPS connections (and uses the same encryption engine in the browser). This prevents third parties from snooping on the data being transferred.
- Input Filtering: Data that enters the flexperto service platform is filtered for malicious content as soon as possible. Data has to process a three-tier security metric containing the WAF in the first stage, followed by an application input validation process and ends on a final validation on database level
- Output Filtering: Data that leaves the flexperto service platform is filtered for malicious content as late as possible. Data has to process a two-tier security metric containing an application input validation process followed by the WAF in the second stage before delivered to the customer.

WebRTC Authentication

Flexperto and TokBox use a secure, token-based technique to authenticate Users in the systems and across Services. Tokens are based on RFC 7591, generated using HMAC256 of relevant API secret and associated with metadata. The following Services take part in this CallFlow:

- **S11** flexpertos atlas Service - Obtains Streaming Tokens from Tokbox (authenticating via API-Key/Secret) for authentic flexperto User Tokens
- **S06** flexpertos web application - Issues and authentications User Tokens in the flexperto realm
- Tokbox AAA Service - Issues and authenticates Tokbox Streaming Tokens
- Tokbox Media Service - Handle Stream negotiation and transport for authentic Tokbox Streaming Tokens

The following CallFlow diagram illustrates the authentication flow for a client that wants to publish a Stream, or subscribe to a Stream within a Session:


Customer - Browser Client
flexperto - WebApplication
flexperto - Atlas Service
Tokbox - AAA Service
Tokbox - Media Service
Username Password Authentication
Returns Authentication Token
Submits Authentication Token
Verifies Authentication Token
Service to Service Authentication (API-Key/Secret)
Obtain User Based Streaming Token
Establish Streaming with User Based Streaming Token

10. Encryption

Encryption measures and processes transform a human or machine readable text/information (cleartext) into an illegible, not easily interpretable representation of the text/information (ciphertext) by the means of an encryption method (cryptosystem). The objective of encryption measurements and processes in flexperto is to protect both the confidentiality and integrity of sensitive and personal data in the cause of an unauthenticated or unauthorized access. In order to protect your customers and enterprise data, flexperto encrypts all data in flight originating from the requesting entity up to the responding entity. The encryption of data in flight is ensured from end to end. The following processes and controls are in place:

- **Public access** to the flexperto network is gatewayed by a LoadBalancer, which performs TLS encryption for public traffic. flexperto currently classifies the following ciphers as secure, and uses them for TLS encryption:
    - ECDHE_RSA_WITH_AES_256_GCM_SHA384
    - ECDHE_RSA_WITH_AES_128_GCM_SHA256
    - ECDHE_RSA_WITH_AES_256_CBC_SHA384
    - ECDHE_RSA_WITH_AES_256_CBC_SHA256

- **Terminal access** is secured via SSH connections. For symmetric encryption, flexperto currently classifies the following ciphers as secure:
  - AES128-CTR
  - AES192-CTR
  - AES256-CTR
- For Host Key Algorithms of SSH Terminal connections, flexperto currently classifies the following ciphers as secure:
  - ECDSA-SHA2-NISTP256
  - ECDSA-SHA2-NISTP384
  - ECDSA-SHA2-NISTP521
  - SSH-RSA
- For Key Exchange Algorithms of SSH Terminal connections, flexperto currently classifies the following ciphers as secure:
  - ECDH-SHA2-NISTP256
  - ECDH-SHA2-NISTP384
  - ECDH-SHA2-NISTP521
  - DIFFIE-HELLMAN-GROUP14-SHA1
  - DIFFIE-HELLMAN-GROUP-EXCHANGE-SHA256
- For Message Authentication Code Algorithms of SSH Terminal connections, flexperto currently classifies the following ciphers as secure:
  - HMAC-SHA2-256
  - HMAC-SHA2-512
- In addition, Terminal access is secured via a **VPN connection**. For synchronous encryption of VPN connections, flexperto currently classifies the following ciphers as secure:
  - AES128-CBC
  - AES192-CBC
  - AES256-CBC
- For Message Authentication Code Algorithms of **VPN connections**, flexperto currently classifies the following ciphers as secure:
  - HMAC-SHA2-256
  - HMAC-SHA2-512

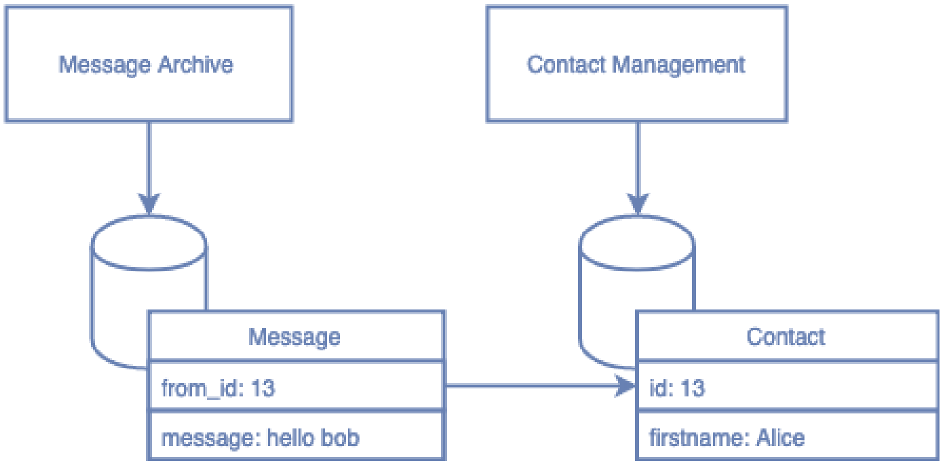
11. Pseudonymization

Pseudonymization measurements of flexperto aim to reduce direct personal reference during data processing in such a way that it is only possible to associate it with a specific data subject if additional information is included. The additional information is being kept separate from the pseudonym by appropriate technical and organizational measures. Pseudonymization measurements of flexperto are enforced during the technical specification process of services within the flexperto platform and software development lifecycle as well as subject to the included peer review. The objectives of pseudonymization are:

- **Migitating harmful consequences of confidentiality breach risks** - By ensuring that service only manages data it requires for fulfilling operating on its business process (concern), in the event of a confidentially breach the scope of the breach is minimized,
- **Ensuring data integrity across the system** - For every data, there is always a single point of truth. Updates to data are centrally authenticated, authorized and managed with the objective to ensure the integrity of the data.
- **Protecting user data in case of compromisation** - Non required User Data is typically not colocated with business data, mitigating the risk of confidentiality breaches of personal data specifically.

- **Reducing Risk of compromisation by minimizing attack vector impact** - The Attack Surface of services is reduced. In order to gain a broad insight on users and business data, typically an introducer has to possess attack vectors against two or more services, increasing the cost of attacks.
- **Enabling Isolation of Security Counter Measurements** - By referencing data across services instead of replicating it, counter measurements on IT-Security Incidents can be minimized in scope and enforced faster. In the case of compromisation, parts of the system can be treated in isolation.
- **Ease of anonymization and erasure** - By referencing personal data instead of replicating it, legal regulations such as the "Right to be forgotten" can easily be complied with since data can be modified easily with immediate global effect.

In order to illustrate the pseudonymization measurements applied within the flexperto platform, find here is a schematic visualization of this principle, with a message sent by Alice:



The Message Archive Service only manages the message (and its body) itself. The identity and personal data of the sender are managed by the separated Contact Management service. Compromisation of either service never discloses a full picture of the business process as it occurred.

12. Access Controls

Flexperto enforces the following controls to ensure that access to your data:

- Are authenticated (Named Persons)
- Are authorized (Are allowed to have access on given data)

Physical Access Controls

Physical Access Controls are measures, which are physically preventing unauthorized persons to access IT-systems and data processing facilities with which personal data are processed.

- 24/7 video surveillance of the outside areas (server location);
- premises protected by a fence with a motion sensor system (server location);
- documented access ID system (server location); and

- 24/7 surveillance by security personnel (server location).

The flexperto office location, while not being a place where your data is processed, is never the less protected via:

- Chipcards, video surveillance and daily access control audit by XXX (Sicherheitsfirma von NG27)
- Management of the chipcards is performed on a per-tenant basis
- Manual locks per area within the location

Electronic Access Controls:

In order to operate and maintain the services, a very limited number of employees (“flexperto Administrators”) are required to be able to access Production Machines.

Role	Data types	Purpose
Flexperto CTO	application logs, user (expert, customer, admin) data, including usernames and encrypted passwords, communication data, content data, meta data	Can have access to this data for maintenance and diagnostic purposes in cases where Administrators/DevOps are not available
Flexperto Administrators/DevOps	application logs, user (expert, customer, admin) data, including usernames and encrypted passwords, communication data, content data, meta data	Can have access to this data for maintenance, diagnostic purposes and 3rd level support in case this is needed
Flexperto Project Management	application logs, user (expert, customer, admin) data	Can have access to this data during the project in terms of the business-cases
Flexperto Customer Support and Success	application logs, user (expert, customer, admin) data	Can have access to this data for project configuration, customer training and 1st/2nd level support
Expert	its customers data	Has access to its customers data

Admin	application logs, user (expert, customer, admin) data	Has access to this data for project configuration and 1st and 2nd level support
Anonymous (not logged in)	published experts profiles data	Has access to expert profile data for experts that published their profile

In order to access the Production Machines, each Authorized Employee is given a unique SSH key. The employee also requires access to the flexperto corporate network. All employees cleared to access the Production Machines are subject to a background check run by or on behalf of flexperto.

flexperto provides up to 24X7 support to Enterprise customers. By its nature, often a very technical, detailed session diagnosis is required to perform root cause analysis. To manage this, regular staff and customer support have access to DB08 and DB09.

Physical Access Controls:

All Production Machines are hosted in a third party data centre. The hosting provider is required to maintain industry best practice security standards. For more details see section 9.

In the general course of business, no employee has physical access to Production Machines as they are located in a third party facility. All on-site maintenance is performed by the hosting provider.

WebRTC Authentication

13. Compliance & Certifications

flexperto requires that all sub-contracted data center and service providers are heaving high security measurements in place.

flexperto service platform

The service provider for hosting the flexperto service platform is velia.net Internetdienste GmbH (Velia). Velia operates several data centers around the world. At the Frankfurt site, Velia operates all servers in cooperation with Telehouse Deutschland GmbH (Telehouse). The Telehouse data center in Frankfurt is certified with ISO 27001 and IDW PS951 (German version of the American SAS70).

flexperto RTC service

The service provider for the RTC service is TokBox inc.. TokBox hosts the application used for the RTC platform in several data centers around the world. Nevertheless, flexperto has made a contractual agreement to use the regional routing functionality of TokBox and thus process and store any data only inside Germany is operated by AWS and ISO 27001 certified.

For the processing of personal data in the USA, flexperto has contracted TokBox Inc. via the so-called standard contract clauses to comply with the protection level of the European Data Protection Directive 95/46 / EC and has sufficient guarantees with regard to the protection of the personality right.

14. Vulnerability and Risk-Assessment

Beyond Vulnerability-Management, flexperto tries to constantly assess possible vulnerability and risks underneath the service layer and implement Countermeassurements. These are:

Are the servers manufacturer requirements for installation and operation met?

All servers are placed within a ISO 27001 datacenter.

Power Supply

- Power supply of racks (up to 8kW) with higher scalable options
- N+1 redundant, SUV-supported power-supply with battery backup
- Up to 21MVA uninterrupted power-supply
- Sub-distribution according to the customer's parameters featuring a separated power-measurement
- Possibility to revert to generators for up to 3 days in case of a power-cut

Environment and air conditioning

- Redundant air conditioning and cooling systems at N1
- Room temperature is kept at 24°C 2/- 4°C
- Temperatures in the datacenters are being monitored by sensors
- Relative air humidity between 50% and 15%
- Floor's carrying capacity between 5 and 15 kN / m2
- Double floors between 300 and 700 mm

Fire detection and extinction systems

- Active inner fire extinction systems
- Visual / thermal fire detectors on two levels (Ceiling and double floor)

Security systems

- Video monitoring of outdoor areas including data recording up to 3 months
- The property is surrounded by a fence with a safety system
- 24/7 control centre on site – Errors are being reported through a centralised control system
- 24/7 security staff on site
- Strict admission process

Are users (including the representants) of IT-systems specifically trained for the tasks?

Every employee receives a thorough introduction to the IT-systems and applications upon the start of his or her employment, unless the knowledge of standard software cannot be assumed to be known.

Every employee will also receive an introduction to the handling of the applications, especially with regards to the data protection factors, by another employee from the same department.

Is data being stored regularly?

All data bases on servers are being stored within a Backup-Strategy.

Are backup devices / device parts available in order to facilitate a smooth replacement?

Limited essential hardware is being provided in case of a necessary replacement. Hardware disks for RAID-Systems are being provided permanently.

Is usage of the IT system only possible after entering an individual user recognition as well as a password authentication?

Each of the IT systems is only accessible after entering an individual username and the respective password. Access to personal data without previous authentication is not possible. Access to a server is only permitted with a personalized SSH2-RSA 2048bit secured key. Those keys are being updated regularly and, in case of termination of an employee's contract, deleted immediately. Further, data that is being processed as part of a mandate is only accessible to a very limited circle of people.

Are sufficient numbers of representatives of the IT administrators available?

Currently, there are two administrators in place. In case of absence (due to illness or holiday leave), another skilled employee who has been trained in the usage of the IT systems will take over.

Who has access to the software?

Access authority is in general only provided to employees who specifically need the relevant applications for their work. In case these prove not to be sufficient, further access to more applications can be granted to the employee.

Are IT systems located in a way that prevents visitors from obtaining any printed or physical information?

As part of our IT guideline, employees are required to arrange their workplaces in a way that prevents visitors from gaining access to any information and personal data.

Are the service provider's activities (e.g. installation, maintenance) being monitored and recorded?

Maintenance of servers is conducted by the hosting service provider without flexperto being present. Maintenance of IT applications or clients is, if possible, conducted by a flexperto employee.

15. Backup-Strategy

Every machine within the flexperto Realm is backed up to disk using Bacula, an Open Source Network Backup Solution. The following Backup Policies are in place:

Backup-System	Type	how often	Environment

Bacula	Full	Weekly (Sunday)	Live
Bacula	Diff	Daily	Live
Bacula	Full	Weekly (Sunday)	Staging
Bacula	Diff	Daily	Staging

The backup servers use a dedicated interface to backup existing service, in order to not interfere with regular, user facing network traffic and capacity during backups and recovery. Backup Servers use a Software-RAID for resilience and are placed in a separate fire compartment. Backup Servers are crossed. This means that the backup server in the staging site backs up the live environment since they are part of the data recovery process.

Backups are tool based verified and System-Administrators and DevOps have to restore data quarterly for training purposes.

16. FAQs

We try to document our platform in such a way that all your questions are answered. Nevertheless sometimes additional questions are raised. And here are the answers for them:

Is a technical Protocol of a Penetration-Test / Data Privacy Audit available?

Possibly. While flexperto does not initiate Penetration-Tests and Data Privacy Audits on a regular basis, flexperto is regularly audited by its customers instead. We believe that these kind of tests where a third party (that is NOT under our span of influence) is penetrating and auditing our work is closer to a real world environment. On the other hand this also means that the technical report of these Tests and Audits is the Intellectual Property of our customers. What we can offer you is to approach us directly, so we can contact you with one of our customers who might publish their report to you and also share their first person experience and impression regarding flexperto’s security and relation to this area of interest.

Is there a Vulnerability Management in place?

Yes there is. Besides the patch management we regularly test our services using OpenVAS (open source version of Nessus).

Which services are provided by vendors / subcontractors?

The RTC-Service is provided by TokBox inc. Their hosting partner is AWS, whose datacenter for this particular service is located in Frankfurt, Germany.

The digital Signature Service is provided in cooperation with Intelligent Solution Services AG.

The server hosting is provided by velia.net Internetdienste GmbH who is using the colocation service provider Telehouse Frankfurt GmbH. All of the servers operated with verlia.net are located in Frankfurt, Germany.

Which Encryption algorithm do you use for hashing passwords?

For hashing passwords and tokens, we use salted SHA256 hashes. Tokens, in addition, have expiry dates for the lifetime of the communication session.

Can we see an Excerpt of your logs?

Of course. Given we sign an NDA and you specify which of the above Log-Types in the Data-Bags listed above you want to see, we can provide you with some samples.

Are access-concepts applied within your WebServices?

Yes, for those services that are exposed to the public, access-concepts reside within the service itself.

Are transactions within Users and Systems authenticated at all times?

Yes every transaction is authenticated either via web session cookies or tokens.

Do you support 2 Factor Authentication?

2 Factor Authentication is currently not supported by the system. Approach us directly if this is an immediate need. Implementation is possible.

Do you support external authentication services?

No, currently external authentication services like SAML/OpenID are not supported. Approach us directly if this is an immediate need. Implementation is possible.

Do you limit the amount of failed authentication attempts?

No, we don't. The reason for that is that this is the easiest way to provide a denial of services of the complete application. Thats why after the 3rd failed attempt we display a reCaptcha that has to be fulfilled in addition instead.

Do you allow password resets for User-Accces to areas with increased need of protection?

No, we don't. Password reset/recovery for administrators is not available.

Do you validate System Outputs?

Yes, we do.

Do you validate System Inputs?

Yes, we do.

Do you protocol validation errors of System Input/Output?

Yes, this is part of our Business-Process Monitoring.

Do you prevent output of internal System-Information (Header, Paths, internal IP-Adresses, Versionsnumbers and Product-Names)?

Yes, just browse demo.flexperto.com and take a look at the response Headers for verification.

Are uploaded files stored with randomized names?

Yes. Names are randomized and extensions based on the MIME-Type of the file. MIME-Types are whitelisted.

Can you give us more detail on Screensharing and the involved Plugins?

Audio, Video and Screensharing use the same WebRTC technology for transporting Streams between Users. The implementation of the WebRTC protocols is done and maintained as part of the Browsers Chrome and Firefox. These Implementations are based on the OpenSource WebRTC library (https://webrtc.org/). The following W3C and RFC standards are the foundation for this library:

- https://www.w3.org/TR/webrtc/
- https://www.w3.org/TR/webrtc/#bib-RFC4566
- https://www.w3.org/TR/webrtc/#bib-RFC7064
- https://www.w3.org/TR/webrtc/#bib-RFC7065
- https://tools.ietf.org/html/rfc3264
- https://tools.ietf.org/html/draft-ietf-rtcweb-security-arch-12

Especially Mozilla invest a lot of effort into documenting the WebRTC implementation and technology. These resources can help you to understand how your browsers perform WebRTC Streaming:

- Overview: https://developer.mozilla.org/en-US/docs/Web/API/WebRTC_API#Protocols
- Protocols: https://developer.mozilla.org/en-US/docs/Web/API/WebRTC_API/Protocols
- Signaling: https://developer.mozilla.org/en-US/docs/Web/API/WebRTC_API/Signaling_and_video_calling
- WebRTC Session Lifetime: https://developer.mozilla.org/en-US/docs/Web/API/WebRTC_API/Session_lifetime

Both Chrome and Firefox implement Screensharing as part of their WebRTC implementation. For security reasons, both vendors defined that this feature is turned off by default and web applications that want to use the feature have to build and provide a plugin. The plugin itself only toggles on the screen sharing feature of the browser, which is sth the user can do by himself via the internal configuration pages provided by the browser himself. The Plugins simply provide a more convenient way for a user to enable the browser's feature. The plugins do not implement the ScreenSharing itself. That is done by the browser. Our Screensharing plugins can be downloaded from the plugin stores of Chrome and Firefox and open them with a Text-Editor. They are pure JavaScript.

https://addons.mozilla.org/de/firefox/addon/flexperto-screensharing/

https://chrome.google.com/webstore/search/flexperto?hl=de

Since IE 10+ does not support WebRTC, the nature of the plugin to be installed here is different. Our Streaming Partner Tokbox builds and provides a Plugin for IE that is based on the OpenSource WebRTC library (https://webrtc.org/). The streaming mechanisms and protocols involved here, therefore, are the same as on the ever-green browsers Chrome and Firefox.