Pegasus – Product Description

Contents

List of Tables

List of Figures

Introduction

Pegasus is a world-leading cyber intelligence solution that enables law enforcement and intelligence agencies to remotely and covertly extract valuable intelligence from virtually any mobile device. This breakthrough solution was developed by veterans of elite intelligence agencies to provide governments with a way to address the new communications interception challenges in today's highly dynamic cyber battlefield. By capturing new types of information from mobile devices, Pegasus bridges a substantial technology gap to deliver the most accurate and complete intelligence for your security operations.

Overcoming Smartphone Interception Challenge

The rapidly growing and highly dynamic mobile communications market - characterized by the introduction of new devices, operating systems and applications on virtually a daily basis – requires a rethinking of the traditional intelligence paradigm. These changes in the communications landscape pose real challenges and obstacles that must be overcome by intelligence organizations and law enforcement agencies worldwide:

- Encryption: Extensive use of encrypted devices and applications to convey messages
- Abundance of communication applications: Chaotic market of sophisticated applications, most of which are IP-based and use proprietary protocols
- Target outside interception domain: Targets' communications are often outside the organization's interception domain or otherwise inaccessible (e.g., targets are roaming, face-to-face meetings, use of private networks, etc.)
- Masking: Use of various virtual identities which are almost impossible to track and trace
- SIM replacement: Frequent replacement of SIM cards to avoid any kind of interception
- Data extraction: Most of the information is not sent over the network or shared with other parties and is only available on the end-user device
- Complex and expensive implementation: As communications become increasingly complex, more network interfaces are needed. Setting up these interfaces with service providers is a lengthy and expensive process, and requires regulation and standardization

Standard Interception Solutions Are Not Enough

Until the above mentioned challenges are addressed and resolved, criminal and terrorist targets are likely "safe" from standard and legacy interception systems, meaning that valuable intelligence is being lost. These standard solutions (described in the sections below) deliver only partial intelligence, leaving the organizations with substantial intelligence gaps.

Passive Interception

Passive interception requires very deep and tight relationships with local service providers (cellular, Internet and PSTN providers) and traditionally has allowed for proper monitoring of text messages and voice calls. However, most contemporary communications is comprised of IP-based traffic, which is extremely difficult to monitor with passive interception due to its use of encryption and proprietary protocols.

Even when this traffic is intercepted, it typically carries massive amounts of technical data that is not related to the actual content and metadata being communicated. Not only does this result in frustrated analysts and wasted time wading through irrelevant data, it also provides a partial snapshot (at best) of the target's communications. In addition, the number of interfaces required to cover the relevant service providers broadens the circle of entities exposed to sensitive information and increases the chance of leakage.

Tactical GSM Interception

Tactical GSM interception solutions effectively monitor voice calls and text messages in GSM networks. When advanced cellular technologies are deployed (3G and LTE networks), these solutions become less efficient. In such cases, it is required to violently downgrade the target to a GSM-based network, which noticeably impacts the user experience and functionality.

These solutions also require a well-trained field tactical team located near the monitored target. Thus, in the majority of cases where the target location is unknown, these solutions become irrelevant. In other cases, placing a tactical team close to the target may pose serious risk both to the team and to the entire intelligence operation.

Malicious Software (Malware)

Malware presumably provides access to the target's mobile device. However, it is not completely transparent and requires the target's involvement to be installed on their devices. This type of engagement usually takes the form of multiple confirmations and approvals before the malware is functional. Most targets are unlikely to be fooled into cooperating with malware due to their high level of sensitivity for privacy in their communications.

In addition, such malware is likely to be vulnerable to most commercially available anti-virus and anti-spyware software. As such, they leave traces and are fairly easily detected on the device.

Cyber Intelligence for the Mobile World

Pegasus is a world-leading cyber intelligence solution that enables law enforcement and intelligence agencies to remotely and covertly extract valuable intelligence from virtually any mobile device. This breakthrough solution was developed by veterans of elite intelligence agencies to provide governments with a way to address the new communications interception challenges in today's highly dynamic cyber battlefield.

By capturing new types of information from mobile devices, Pegasus bridges a substantial technology gap to deliver the most accurate and complete intelligence for your security operations. This solution is able to penetrate the market's most popular smartphones based on BlackBerry, Android, iOS and Symbian operating systems.

Pegasus silently deploys invisible software ("agent") on the target device. This agent then extracts and securely transmits the collected data for analysis. Installation is performed remotely (over-the-air), does not require any action from or engagement with the target, and leaves no traces whatsoever on the device.

Benefits of Pegasus

Organizations that deploy Pegasus are able to overcome the challenges mentioned above to achieve unmatched mobile intelligence collection:

- Unlimited access to target's mobile devices: Remotely and covertly collect information about your target's relationships, location, phone calls, plans and activities – whenever and wherever they are
- Intercept calls: Transparently monitor voice and VoIP calls in real-time
- Bridge intelligence gaps: Collect unique and new types of information (e.g., contacts, files, environmental wiretap, passwords, etc.) to deliver the most accurate and complete intelligence
- Handle encrypted content and devices: Overcome encryption, SSL, proprietary protocols and any hurdle introduced by the complex communications world
- Application monitoring: Monitor a multitude of applications including Skype, WhatsApp, Viber, Facebook and Blackberry Messenger (BBM)
- Pinpoint targets: Track targets and get accurate positioning information using GPS
- Service provider independence: No cooperation with local Mobile Network Operators (MNO) is needed
- Discover virtual identities: Constantly monitor the device without worrying about frequent switching of virtual identities and replacement of SIM cards
- Avoid unnecessary risks: Eliminate the need for physical proximity to the target or device at any phase

Technology Highlights

The Pegasus solution utilizes cutting-edge technology specially developed by veterans of intelligence and law enforcement agencies. It offers a rich set of advanced features and sophisticated intelligence collection capabilities not available in standard interception solutions:

- Penetrates Android, BlackBerry, iOS and Symbian based devices

- Extracts contacts, messages, emails, photos, files, locations, passwords, processes list and more
- Accesses password-protected devices
- Totally transparent to the target
- Leaves no trace on the device
- Minimal battery, memory and data consumption
- Self-destruct mechanism in case of exposure risk
- Retrieves any file from the device for deeper analysis

High Level Architecture

The Pegasus system is designed in layers. Each layer has its own responsibility forming together a comprehensive cyber intelligence collection and analysis solution.

The main layers and building blocks of the systems are:

- Installations: The Installation layer is in charge of issuing new agent installations, upgrading and uninstalling existing agents.
- Data Collection: The Data Collection layer is in charge of collecting the data from the installed device. Pegasus offers comprehensive and complete intelligence by employing four collection methods:
  - Data Extraction: Extraction of the entire data that exists on the device upon agent installation
  - Passive Monitoring: Monitor new arrival data to the device
  - Active Collection: Activate the camera, microphone, GPS and other elements to collect real-time data
  - Event-based Collection: Define scenarios that automatically triggers specific data collection
- Data Transmission: The Data Transmission layer is in charge of transmitting the collected data back to the command and control servers, using the most efficient and safe way.
- Presentation & Analysis: The Presentation & Analysis component is a User Interface that is in charge of presenting the collected data to the operators and analysts, turning the data into actionable intelligence. This is done using the following modules:
  - Real-Time Monitoring: Presents real-time collected data from specific or multiple targets. This module is highly important when dealing with sensitive targets or during operational activities, where each piece of information that arrives is crucial for decision making.
  - Offline Analysis: Advanced queries mechanism that allows the analysts to query and retrieve any piece of information that was collected. The advanced mechanism provides tools to find hidden connections and information.
  - Geo-based Analysis: Presents the collected data on a map and conduct geo-based queries.
  - Rules & Alerts: Define rules that trigger alerts based on specific data that arrives or event that occurred.
- Administration: The administration component is in charge of managing the entire system permission, security and health:

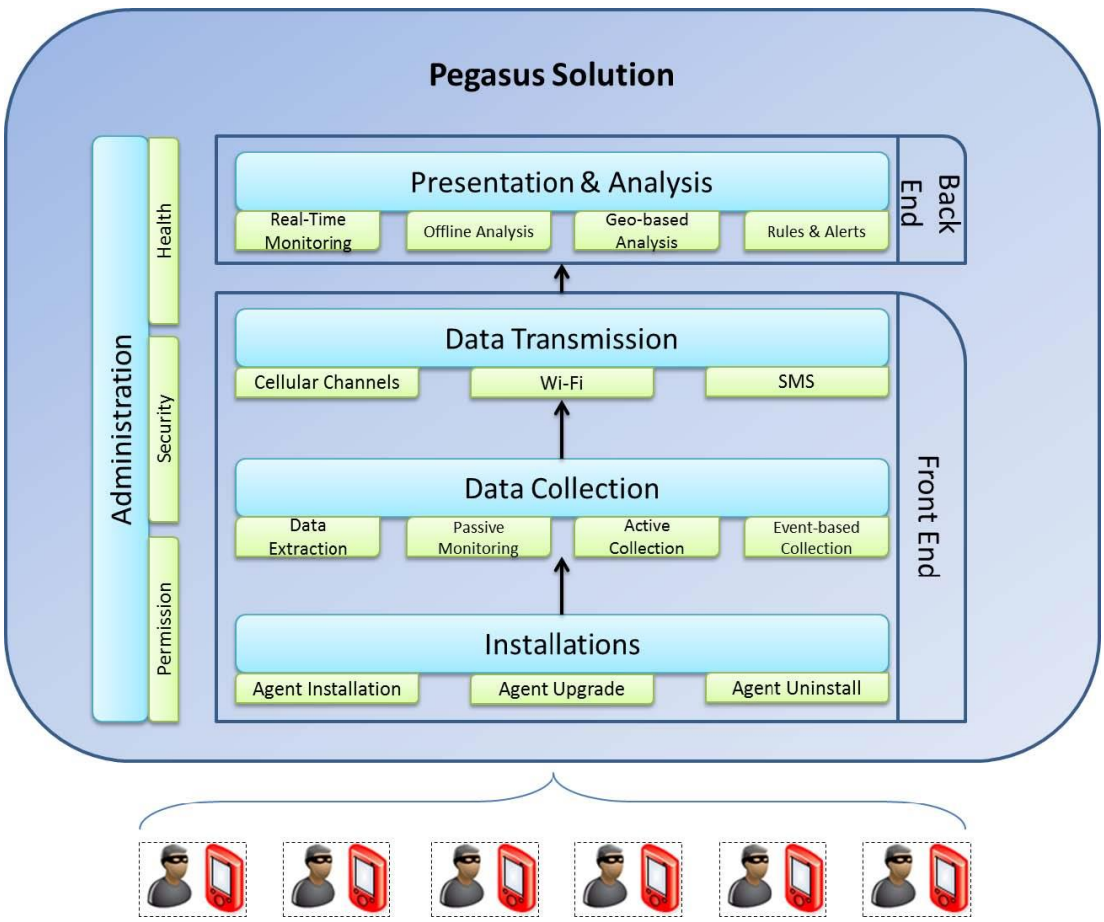
– Permission: The permissions mechanism allows the system administrator to manage the different users of the system. Provide each one of them the right access level only to the data they are allowed to. This allows to define groups in the organization that handle only one or more topics and other groups which handles different topics.

– Security: The security module monitors the system security level, making sure the collected data is inserted to the system database clean and safe for future review.

– Health: The health component of the Pegasus solution monitor the status of all components making sure everything is working smoothly. It monitors the communication between the different parts, the system performance, the storage availability and alerts if something is malfunction.

The system layers and components are shown in Figure 1.

Figure 1: Pegasus High Level Architecture



Agent Installation

In order to start collecting data from your target's smartphone, a software based component ("Agent") must be remotely and covertly installed on their device.

Agent Purpose

The "Agent", a software based component, resides on the end point devices of the monitored targets and its purpose is to collect the data it was configured to. The agent is supported on the most popular operating systems: BlackBerry, Android, iOS (iPhone) and Symbian based devices.

Each agent is independent and is configured to collect different information from the device and to transmit it via specific channels in defined timeframes. The data is sent back to the Pegasus servers in a hidden, compressed and encrypted manner.

The agent continuously collects the information from the device and will transmit it once reliable internet connection becomes available.

Communications encryption, the use of many applications and other communications concealing methods are no longer relevant when an agent is installed on the device.

Agent Installation Vectors

Injecting and installing an agent on the device is the most sensitive and important phase of intelligence operation conducted on the target device. Each installation has to be carefully planned to ensure it is successful. The Pegasus system supports various installation methods. The installation methods variety answers the different operational scenarios which are unique to each customer, resulting in the most comprehensive and flexible solution. Following are the supported installation vectors:

Remote Installation (range free):

- Over-the-Air (OTA): A push message is remotely and covertly sent to the mobile device. This message triggers the device to download and install the agent on the device. During the entire installation process no cooperation or engagement of the target is required (e.g., clicking a link, opening a message) and no indication appears on the device. The installation is totally silent and invisible and cannot be prevented by the target. This is NSO uniqueness, which significantly differentiates the Pegasus solution from any other solution available in the market.

- Enhanced Social Engineering Message (ESEM): In cases where OTA installation method is inapplicable[1], the system operator can choose to send a regular text message (SMS) or an email, luring the target to open it. Single click, either planned or unintentional, on the link will result in hidden agent installation. The installation is entirely concealed and although the target clicked the link they will not be aware that software is being installed on their device.

  The chances that the target will click the link are totally dependent on the level of

1 e.g., some devices do not support it; some service providers block push messages; target phone number in unknown.

content credibility. The Pegasus solution provides a wide range of tools to compose a tailored and innocent message to lure the target to open the message.

NOTE: Both OTA and ESEM methods require only a phone number or an email address that is used by the target. Nothing else is needed in order to accomplish a successful installation of the Pegasus agent on the device.

Close to the target (range limited):

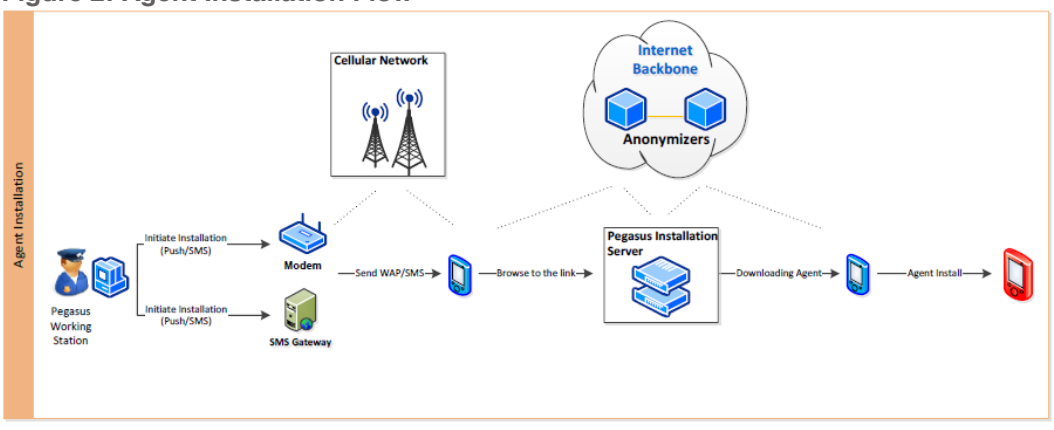
- Tactical Network Element: The Pegasus agent can be silently injected once the number is acquired using tactical network element such as Base Transceiver Station (BTS). The Pegasus solution leverages the capabilities of such tactical tools to perform a remote injection and installation of the agent. Taking a position in the area of the target is, in most cases, sufficient to accomplish the phone number acquisition. Once the number is available, the installation is done remotely.
- Physical: When physical access to the device is an option, the Pegasus agent can be manually injected and installed in less than five minutes. After agent installation, data extraction and future data monitoring is done remotely, providing the same features of any other installation method.

NOTE: Tactical and Physical installations are usually used where no target phone number or email address are available.

Agent Installation Flow

Remote agent installation flow is shown in Figure 2.

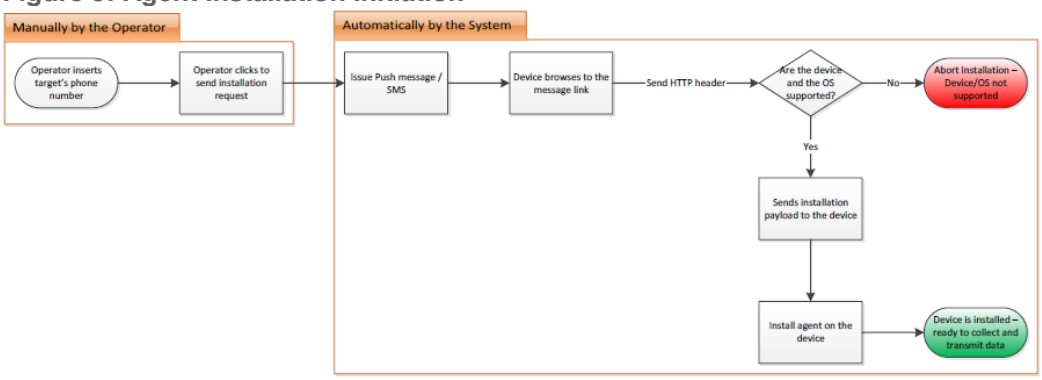
Figure 2: Agent Installation Flow



In order to initiate a new installation, the operator of the Pegasus system should only insert the target phone number. The rest is done automatically by the system, resulting in most cases with an agent installed on the target device.

Agent installation initiation is shown in Figure 3.

Figure 3: Agent Installation Initiation



Supported Operating Systems & Devices

Operating System (OS)	OS Version	Device	Comments
Android	2.1 – 4.2	▪ Samsung Galaxy series ▪ Sony Ericsson Xperia series ▪ Others (refer to note below)	Support is based on local firmware versions, which must be defined with the customer
iOS	4.x – 6.1.4	▪ iPhone 4 ▪ iPhone 4S ▪ iPhone 5	
BlackBerry	5.0 – 7.1	▪ Curve (8520, 9300, 9350, 9360) ▪ Bold (9000, 9700, 9780, 9790, 9900, 9930) ▪ Torch (9800, 9810, 9850, 9860) ▪ Pearl (9100)	
Symbian	Version S60 OS9 3rd edition FP1, FP2, 5th edition and Symbian^3	Variety of devices	Support is based on local firmware versions, which must be defined with the customer

NOTE: Android-based devices are often added to the supported list. An updated list can be sent upon customer request.

Installation Failure

The installation can sometimes fail due to following reasons:

1. Unsupported device: the target device is not supported by the system (which appears above).

2. Unsupported OS: the operating system of the target device is not supported by the system.

3. Unsupported browser: the default browser of the device was previously replaced by the target. Installation from browsers other than the device default (and also Chrome for Android based devices) is not supported by the system.

In any of the above mentioned cases, if the operator initiates a remote installation to a non-supported device, operating system or browser, the injection will fail and the installation will be aborted. In these cases the process is finished with an open browser on the target device pointing and showing the URL page which was defined by the operator prior the installation.

The device, OS and browser are identified by the system using their HTTP user agent. If by any reason the user agent was manipulated by the target, the system might fail to correctly identify the device and OS and provide the wrong installation payload. In such case, the injection will fail and the installation will be aborted, showing again the above mentioned URL page.

Data Collection

Upon successful agent installation, a wide range of data is monitored and collected from the device:

- Textual: Textual information includes text messages (SMS), Emails, calendar records, call history, instant messaging, contacts list, browsing history and more. Textual information is usually structured and small in size, therefore easier to transmit and analyze.
- Audio: Audio information includes intercepted calls, environmental sounds (microphone recording) and other audio recorded files.
- Visual: Visual information includes camera snapshots, photos retrieval and screen capture.
- Files: Each mobile device contains hundreds of files, some bear invaluable intelligence, such as databases, documents, videos and more.
- Location: On-going monitoring of the device location (Cell-ID and GPS).

The variety of data that is collected by the Pegasus system is shown in Figure 4.

Figure 4: Collected Data

The data collection is divided into three levels:

- Initial data extraction
- Passive monitoring
- Active collection

Initial Data Extraction

Once the agent is successfully injected and installed on the device, the following data that resides and exists on the device can be extracted and sent to the command and control center:

- SMS records
- Contacts details
- Call history (call log)
- Calendar records
- Emails
- Instant Messaging
- Browsing history

As opposed to other intelligence collection solutions which provide only future monitoring of partial communications, Pegasus allows the extraction of all existing data on the device. As a result the organization benefits from accessing historical data about the target, which assists in building a comprehensive and accurate intelligence picture.

NOTE: Initial data extraction is an option and not a must. If the organization is not allowed to access historical data of the target, such option can be disabled and only new arrival data will be monitored by the agent.

Passive Monitoring

From the point the agent was successfully installed it keeps monitoring the device and retrieves any new record that becomes available in real-time (or at specific condition if configured differently). Below is the full list of data that is monitored by the agent:

- SMS records
- Contacts details
- Call history (call log)
- Calendar records
- Emails
- Instant Messaging
- Browsing history
- Location tracking (Cell-ID based)

Active Collection

In addition to passive monitoring, upon successful agent installation a wide set of active collection features becomes available. Active collection refers to active requests sent by the operator to collect specific information from the installed device. These set of features are called active, as they carry their collection upon explicit request of the operator. Active collection allows the operator to perform real-time actions on the target device, retrieving unique information from the device and from the surrounding area of the target, including:

- Location tracking (GPS based)

- Voice calls interception
- File retrieval
- Environmental sound recording (microphone recording)
- Photo taking
- Screen capturing

Active collection differentiates Pegasus from any other intelligence collection solution, as the operator controls the information that is collected. Instead of just waiting for information to arrive, hoping this is the information you were looking for, the operator actively retrieves important information from the device, getting the exact information he was looking for.

Description of Collected Data

The different types of data available for extraction, passive monitoring and active collection with their respective features are listed in Table 1.

Table 1: Collection Features Description

Application Type	Features Description	Data Extraction	Passive / Active Collection
Instant Messaging (IM): 1. WhatsApp 2. Viber 3. Skype 4. BlackBerry Messenger (BBM)	Agent extracts and monitors all the incoming and outgoing instant messages to/from the device. Full 1-on-1 conversation extraction and monitoring including group chat. Indication for file transfer (file name).	✔	✔
Location Tracking	The system provide two types of location information about the device: GPS: 1. Upon user request, a defined timeframe for sampling location is opened. GPS data is retrieved when applicable (available reception). In case GPS signal is not accessible, Cell-ID is retrieved. 2. If GPS is disabled by the target, the system enable it for sampling and immediately turn it off Cell-ID: Devices constantly transmit their location (Cell-ID) every time they communicate with the server. The retrieved location data is analyzed at the server and placed on map. Location-based queries and alerts are easily set.	✔	✔
Calendar	Agent extracts all the calendar records from the device and monitors any change or new event added to the calendar.	✔	✔
Contact details	Agent extracts all contacts available on the device. From this point the agent monitors any change/deletion of existing contacts and the addition of new contact.	✔	✔

Application Type	Features Description	Data Extraction	Passive / Active Collection
	The agent extracts and monitors all values assigned in each contact field that is available (based on vCard fields), including photo if assigned.		
Environmental sound recording (microphone recording)	The user can request to turn on the device microphone and listen in real-time to the surrounding sounds. The surrounding sounds are recorded and can be analyzed and replayed at a later stage. Turning on the microphone is based on an incoming silent call to the device from the server (PBX). Such call is allowed only after the agent assured that the device is in idle mode (device is not in active use and the screen is turned off). Any action by the target that turns on the screen will result in immediate call hang-up and cease of capturing surrounding sounds. No indication of the recording or the incoming silent call appears on the device at any point. The quality of the recording depends on the device's microphone sensitivity, the surrounding noise and the device model. This sensitivity varies between the different mobile phone models and is set by the phone manufacturer. Usually the content of a conversation held a few meters next to the device can be heard.	N/A[2]	✔
SMS	Agent extracts and monitors all the incoming and outgoing text messages (SMS).	✔	✔
Call Interception (call recording) – Android only	The user can request to record incoming and outgoing calls of the target device. The calls are recorded locally on the device and then sent to the system servers upon completion.	N/A	✔
Email: 1. Main email application in all platforms 2. Gmail application in Android	Agent extracts and monitors all the emails that reside on the device. The main email application (stock) on the device is monitored, thus all accounts which are defined there are monitored (e.g., exchange, Gmail, etc.). For Android-based devices both the main email stock application and the Gmail application are monitored.	✔	✔
File retrieval	Upon user request a full list of files and folders is extracted from the device (internal storage and SD card). When the operator spots a file of interest he can immediately request to retrieve it.	N/A	✔
Photo taking	Upon user request snapshots using the front and rear camera are taken from the device and sent to the servers. The snapshots are taken only after the agent assured that the	N/A	✔

2 For active collection features, initial data is not extracted before a request is initiated by the user.

Application Type	Features Description	Data Extraction	Passive / Active Collection
	device is in idle mode. During photo taking no indication appears on the device and flash is never used. The quality of the photo can be chosen by the operator to reduce data usage and faster photo transmission. Since flash is not used and the phone might be in motion or inside rooms with low light, the photos are sometimes out of focus.		
Screen capturing	Upon user request a screen capture is taken and sent to the Pegasus servers. The device screenshots can provide insights on the applications used by the target, wallpaper image used and more intimate information about the target.	N/A	✔
Browsing history	Agent extracts and monitors the history of browsed websites from the default browser of the device.	✔	✔
Browsing favorites	Agent extracts and monitors the favorites websites saved in the default browser of the device.	✔	✔
Call history (call log)	Agent extracts the history of all incoming/outgoing calls made to/from the device. The data includes the caller and callee numbers and the duration of the call. Calling attempts which did not result with a conversation will show duration of 0 (zero) seconds.	✔	✔
Device information	Upon agent installation all device, network and connection details are extracted to monitor the general information of the device, including battery level. This provides a summarized view to help understand at-a-glance the device status.	✔	✔

The above mentioned data is the potential data that could be collected by an agent. The agent will collect the data that is applicable and available on the device. If one or more of the above mentioned applications does not exist and/or removed from the device, the agent will operate in the same manner. It will collect the data from the rest of the services and applications which are in use in the device. Also, all the collected data from the removed application will still be saved on the servers or at the agent, if it was not yet transmitted back to the servers.

In addition, the above mentioned data that is collected by the agent covers the most popular applications used worldwide. Since applications popularity differs from country to country, we understands that data extraction and monitoring of other applications will be required as time evolves and new applications are adopted by targets. When such requirement is raised, we can fairly easily extract the important data from virtually any application upon customer demand and release it as a new release that will become available to the customer.

Collection Buffer

The installed agent monitors the data from the device and transmits it to the servers. If transmission is not possible[3] the agent will collect the new available information and transmits it when connection will become available. The collected data is stored in a hidden and encrypted buffer. This buffer is set to reach no more than 5% of the free space available on the device. For example – if the monitored device has 1GB of free space, the buffer can store up to 50MB. In case the buffer has reached its limit, the oldest data is deleted and new data is stored (FIFO). Once the data has been transmitted, the buffer content is totally deleted.

3 No data channels are available; Device is roaming; Device is shut down.

Data Transmission

By default, the collected data (initial data extraction, passive monitoring and active collection) is sent back to the command and control center in real-time. The data is sent via data channels, where Wi-Fi is the preferred connection to use when it is available. In other cases data is transmitted via cellular data channels (GPRS, 3G and LTE). Extra thought was put into compression methods and focusing on textual content transmission whenever possible. The data footprints are very small and usually take only few hundred bytes. This is to make sure that the collected data is easily transmitted, ensuring minimal impact on the device and on the target cellular data plan.

If data channels are not available, the agent will collect the information from the device and store it in a dedicated buffer, as explained in Data Collection section.

Data transmission is automatically ceased in the following scenarios:

- Low battery: When the device battery level is below the defined threshold (5%) all data transmission processes are immediately ceased until the device is recharged.
- Roaming device: When the device is roaming, cellular data channels become pricy, thus data transmission is done only via Wi-Fi. If Wi-Fi does not exist, transmission will be ceased.

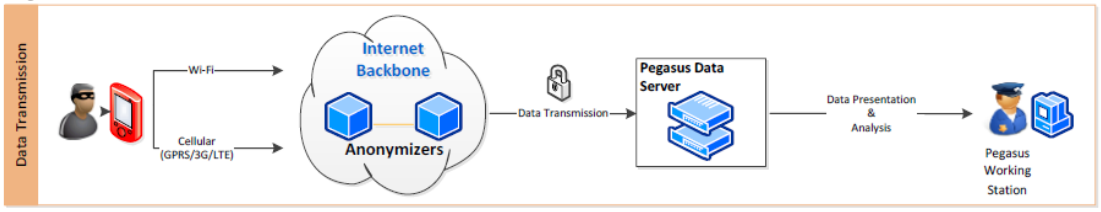
When no data channels are available, and no indication for communication is coming back from the device, the user can request the device will communicate and/or send some crucial data using text messages (SMS).

CAUTION: Communication and/or data transmission via SMS may incur costs by the target and appear in his billing report thus should be used sparingly.

The communication between the agent and the central servers is indirect (through anonymizing network), so trace back to the origin is non-feasible.

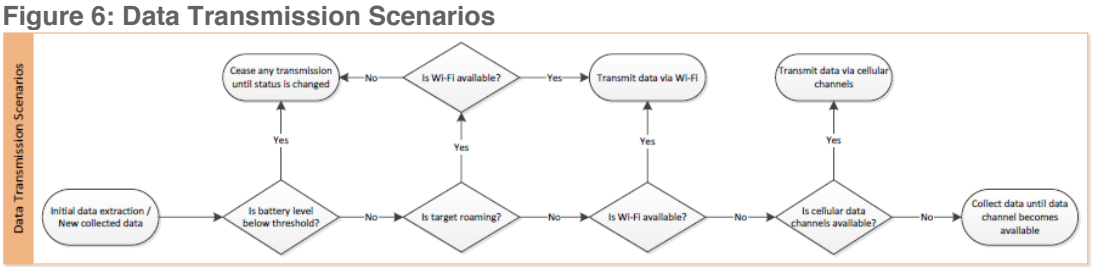
The Pegasus system data transmission process is shown in Figure 5.

Figure 5: Data Transmission Process



The channels and scenarios for transmitting the collected data are shown in Figure 6.

Figure 6: Data Transmission Scenarios



Data Transmission Security

All connections between the agents and the servers are encrypted with strong algorithms and are mutually authenticated. While data encryption is probably the most urging issue, extra care was given to ensure minimal data, battery and memory are consumed within the agents requirements. This is meant to make sure that no concerns are raised by the target.

Detecting an operating agent by the target is almost impossible. The Pegasus agent is installed at the kernel level of the device, well concealed and is untraceable by antivirus and antispy software.

The transmitted data is encrypted with symmetric encryption AES 128-bit.

Pegasus Anonymizing Transmission Network

Agent transparency and source security are the guiding principles of the Pegasus solution. To assure that trace back to the operating organization is impossible, the Pegasus Anonymizing Transmission Network (PATN), a network of anonymizers is deployed to serve each customer. The PATN nodes are spread in different locations around the world, allowing agent connections to be redirected through different paths prior to reaching the Pegasus servers. This ensures that the identities of both communicating parties are highly obscured.

Data Presentation & Analysis

Successful data collection from hundreds of targets and devices generates massive amounts of data for visualization, presentation and analysis. The system provides a set of operational tools to help the organization to transform data into actionable intelligence. This is to view, sort, filter, query and analyze the collected data. The tools include:

- Geographical analysis: Track target's real-time and historical location, view several targets on map
- Rules and alerts: Define rules to generate alerts upon important data arrival
- Favorites: Mark important and favorite events for subsequent review and deeper analysis
- Intelligence dashboard: View highlights and statistics of target's activities
- Entity management: Manage targets by groups of interest (e.g., drugs, terror, serious crime, location, etc.)
- Timeline analysis: Review and analyze collected data from a particular time frame
- Advanced search: Conduct search for terms, names, code words and numbers to retrieve specific information

The collected data is organized by groups of interest (e.g., drugs group A, terror group B, etc.) and each group consists of targets. Each target consists of several devices which some have installed agents on them.

The collected data is displayed in an easy-to-use intuitive user interface and when applicable emulates popular display of common applications. The intuitive user interface is designed for a day-to-day work. Operators can easily customize the system to fit their preferred working methods, define rules and alerts for specific topics of interest.

The operator can choose to view the entire collected data from specific target or only specific type of information such as location information, calendar record, emails or instant messages.

Pegasus calendar monitoring screen is shown in Figure 7.

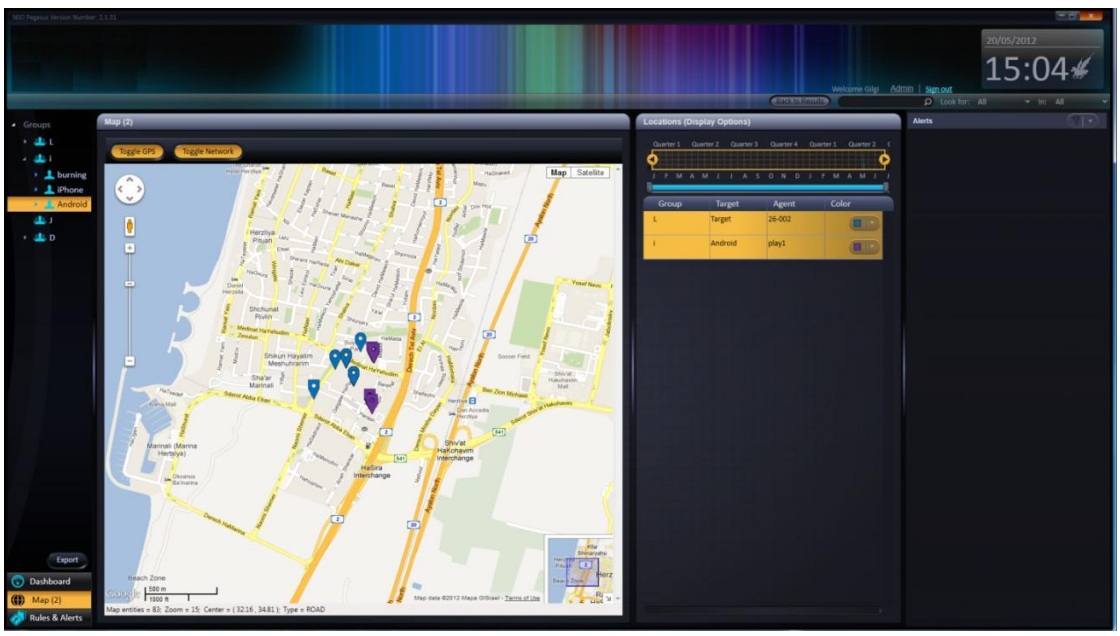
Figure 7: Calendar Monitoring

Pegasus call log and call interception screen is shown in Figure 8.

Figure 8: Call Log & Call Interception

Pegasus location tracking screen is shown in Figure 9.

Figure 9: Location Tracking



The presentation fields of the collected data are listed in Table 2.

Table 2: Presentation of Collected Data

Service / Application Type	Extracted data	Display method
Instant Messaging (IM): 1. WhatsApp 2. Viber 3. Skype 4. BlackBerry Messenger (BBM)	▪ Chat participants (Names & phones) ▪ Conversation content ▪ Date & Time ▪ Attachments metadata (without the attachment)	▪ Grid ▪ Conversation mode
Location Tracking	▪ Data source (GPS/Cell-ID) ▪ Latitude ▪ Longitude ▪ Date & Time	▪ Grid ▪ Map: - On map display - Full trail - Type of location data (GPS or Cell-ID based)
Calendar	▪ Meeting subject ▪ Event date and start time	▪ Grid ▪ Monthly calendar view (emulates popular calendar clients)
Contact details	▪ Entire values stored in the contact entry including photo if available	▪ Grid ▪ Contact card with the entire details
Environmental sound recording (microphone recording)	▪ Recorded audio ▪ Recording Date & Time ▪ Duration	▪ Grid ▪ Playback interface
SMS	▪ Direction (incoming, outgoing) ▪ Contact name ▪ Phone number ▪ Message content ▪ Date & Time	▪ Grid
Call Interception	▪ Direction ▪ Contact name ▪ Phone number ▪ Duration ▪ Date & Time	▪ Grid ▪ Playback interface
Email: 1. Main email application in all platforms 2. Gmail application in Android	▪ From ▪ To ▪ CC ▪ BCC ▪ Subject ▪ Folder ▪ Account ▪ Message content ▪ Date & Time	▪ Grid ▪ HTML (emulates popular email clients)
File retrieval	▪ List of folders (tree) ▪ List of files (grid): ▪ Filename	▪ Grid ▪ Tree view

Service / Application Type	Extracted data	Display method
	▪ Modified date ▪ File size	
Photo taking	▪ Date & Time ▪ Photo	▪ Grid ▪ Photo viewer
Screen capturing	▪ Date & Time ▪ Screen capture image	▪ Grid ▪ Photo viewer
Browsing history	▪ Website name (as saved by the target, usually the default website name) ▪ Website URL address	▪ List
Browsing favorites	▪ Website name (as saved by the target, usually the default website name) ▪ Website URL address	▪ List
Call history (call log)	▪ Direction ▪ Contact name ▪ Phone number ▪ Duration ▪ Date & Time	▪ Grid
Device information	▪ Battery level ▪ Connection type (e.g., 3G, WiFi) ▪ MSISDN ▪ IMEI ▪ IMSI ▪ Device Manufacturer ▪ Device model ▪ Operating System version ▪ Installation date ▪ Last communication time ▪ Device current country ▪ Device home country ▪ Serving network ▪ Home serving network	▪ Dashboard

Rules & Alerts

The Rules & Alerts module in the system alerts when important event takes place. Rules must be defined in advance and they help the operators to review and take actions in real-time, for example:

- Geo-fencing:
  - Access hot zone - Alert when target reached an important location
  - Leave hot zone - Alert when target left a certain location

  Geo-fence alerts are based on a perimeter around a certain location, where the operator defines the size of the perimeter.
- Meeting detection: Alert when two targets meet (share the same location)

- Connection detection:
    - Alert when a message is sent from/to a specific number
    - Alert when a phone call is performed from/to a specific number
- Content detection: Alert when a defined word/term/code word is used in a message

Data Export

The system is designed as an end-to-end system, providing its users with collection and analysis tools. However, we understands that there are advanced analysis capabilities and data fusion requirements from other sources, therefore the system allows the exporting of the collected information and seamless integration with 3rd party backend or analysis systems available.

Agent Maintenance

Once agent is installed on a certain device, it has to be maintained in order to support new features and change its settings and configurations or to be uninstalled when it is no longer providing valuable intelligence to the organization.

Agent Upgrade

When agents' updates are released they become available to install. These new agents are now ready for installation on new targets' devices or as upgrades for existing agents installed on target's devices. These updates provide new functionalities, bug fixing, support for new services or improve the agents overall behavior. Such updates are crucial to keep the agent functional and operational in the endless progress of the communication world and especially the smartphone arena.

There are two types of agent upgrades:

- Optional upgrade: agent upgrade is not mandatory by the system. The user decides when, if at all, to upgrade the agent.
- Mandatory upgrade: agent upgrade is mandatory by the system. The supervisor must upgrade the agent otherwise no new information will be monitored from the device.

Upgrade sometimes requires an installation of a new agent and sometimes just a small update of the existing agent. In both cases the user is the only one to decide when to conduct the upgrade, and therefore should plan this accordingly.

Once the command for upgrade was sent by the user, the process should take only few minutes. The process might take longer if the device is turned off or has bad data connection. In either case, the upgrade will be accomplished once a decent data connection becomes available.

Agent Settings

Agent settings are set for the first time during its installation. From this point, these settings serve the agent, but can always be changed if required. The settings include the IP address for transmitting the collected data, the way commands are sent to the agent, the time until the agent is automatically uninstall itself (see self-destruct mechanism for more details) and more.

Agent Uninstall

When the intelligence operation is done or in case where the target is no longer with interest to the organization, the software based component ("Agent") on the target's device can be removed and uninstalled. Uninstall is quick, requires a single user request and has no to minimal effect on the target device. The user issues a request for agent uninstall which is sent to the device.

Once agent is uninstalled from a certain device it leaves no traces whatsoever or indications it was ever existed there[4]. As long as the agent is operational on the device and a connection exists between him and the servers it can be easily and remotely uninstalled.

Uninstall can always be done remotely no matter what was the method used for installation. Physical uninstall is also an option, if needed.

Uninstalling an agent does not mean losing the entire collected data – the entire data that was collected during the time that the agent was installed on the device will be kept in the servers for future analysis.

Self-Destruct Mechanism

The Pegasus system contains self-destruct mechanism for the installed agents. In general, we understand that it is more important that the source will not be exposed and the target will suspect nothing than keeping the agent alive and working. The mechanism is activated in the following scenarios:

- Risk of exposure: In cases where a great probability of exposing the agent exists, a self-destruct mechanism is automatically being activated and the agent is uninstalled. Agent can be once again installed at a later time.
- Agent is not responding: In cases where the agent is not responding and did not communicate with the servers for a long time[5], the agent will automatically uninstall itself to prevent being exposed or misused.

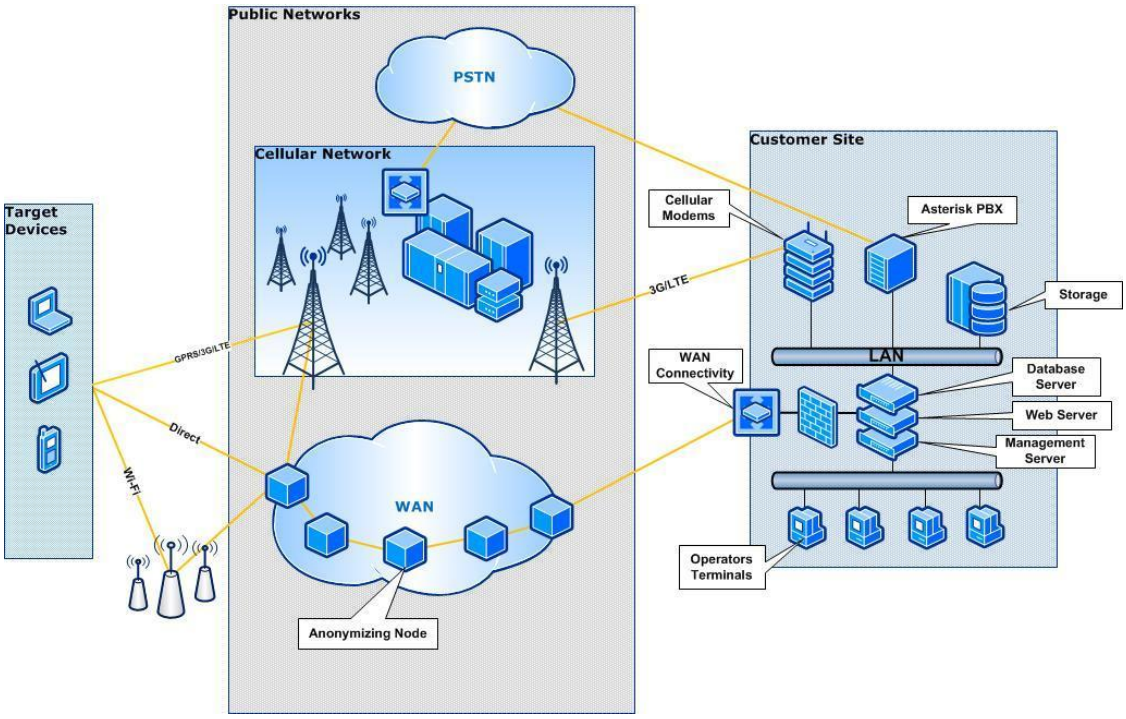
4 In some cases, uninstall can result in device reboot. If reboot takes place, it happens once agent removal is done. The device comes up clean with no agent installed.

5 The default time is 60 days, but can be reconfigured for any period of time required

Solution Architecture

The Pegasus system's major architectural components are shown in Figure 10.

Figure 10: Solution Architecture



Customer Site

NSO is responsible to deploy and configure the Pegasus hardware and software at the customer premises, making sure the system is working and functioning properly. Below are the main components installed at the customer site:

WEB Servers

Residing at the customer's premises, the servers are responsible for the following:

- Agent installation and monitoring
- Agent maintenance: Remotely control, configure and upgrade installed agents
- Data transmission: Receive the collected data transmitted from the installed agents
- Serve the operators' terminals

Communications Module

The communications module allows interconnectivity and internet connection to the servers.

Cellular Communication Module

The cellular communication module enables remote installation of the Pegasus agent to the target device using cellular modems and/or SMS gateways.

Permission Module

The Pegasus permission management module defines and controls the features and available content allowed for each user based on their role, rank and hierarchy.

Data Storage

The collected data that was extracted and monitored by the agents is stored on an external storage device. The data is well backed-up and with full resiliency and redundancy to prevent failures and downtime.

Servers Security

All the servers reside inside the customer's trusted network, behind any security measures it may deploy as well as security measures that we supply specifically for the system.

Hardware

The system standard hardware is deployed on several servers connected together on couple of racks. The equipment takes care of advanced load balancing, content compression, connection management, encryption, advanced routing, and highly configurable server health monitoring.

Operator Consoles

The operator's end-point terminals (PC) are the main tool which the operators activate the Pegasus system, initiate installations and commands, and view the collected data.

Pegasus Application

The Pegasus application is the user interface that is installed on the operator terminal. It provides the operators with range of tools to view, sort, filter, manage and alert to analyze the large amount of data collected from the targets' agents.

Public Networks

Apart from local hardware and software installation at the customer premises, the Pegasus system does not require any physical interface with the local mobile network operators. However, since agent installations and data are transferred over the public networks, we makes sure it is transferred in the most efficient and secured way, all the way back to the customer servers:

Anonymizing Network

Pegasus Anonymizing Transmission Network (PATN) is built from anonymizing connectivity nodes which are spread in different locations around the world, allowing agent connections to be directed through different paths prior to reaching the Pegasus servers. The anonymized nodes serve only one customer and can be set up by the customer if required.

See more information in Pegasus Anonymizing Transmission Network section.

Target Devices

The above mentioned architecture allows the operators to issue new installations, extract, monitor and actively collect data from targets' devices. See more details in Supported Operating Systems & Devices.

NOTE: The Pegasus is an intelligence mission-critical system, therefore it is fully redundant to avoid malfunctions and failures. The system handles large amounts of data and traffic 24 hours a day and is scalable to support customer growth and future requirements.

Solution Hardware

The hardware specifications for operating the Pegasus system depends on the number of concurrent installed agents, the number of working stations, the amount of data stored and for how long should it be stored.

All the necessary hardware is supplied with the system upon deployment and may require local customization that has to be handled by the customer based on we directions. If required, hardware can be purchased by the customer based on the specifications provided by we.

Operators Terminals

The operator terminals are standard desktop PCs, with the following specifications:

- Processor: Core i5
- Memory: 3GB RAM
- Hard Drive: 320GB
- Operating System: Windows 7

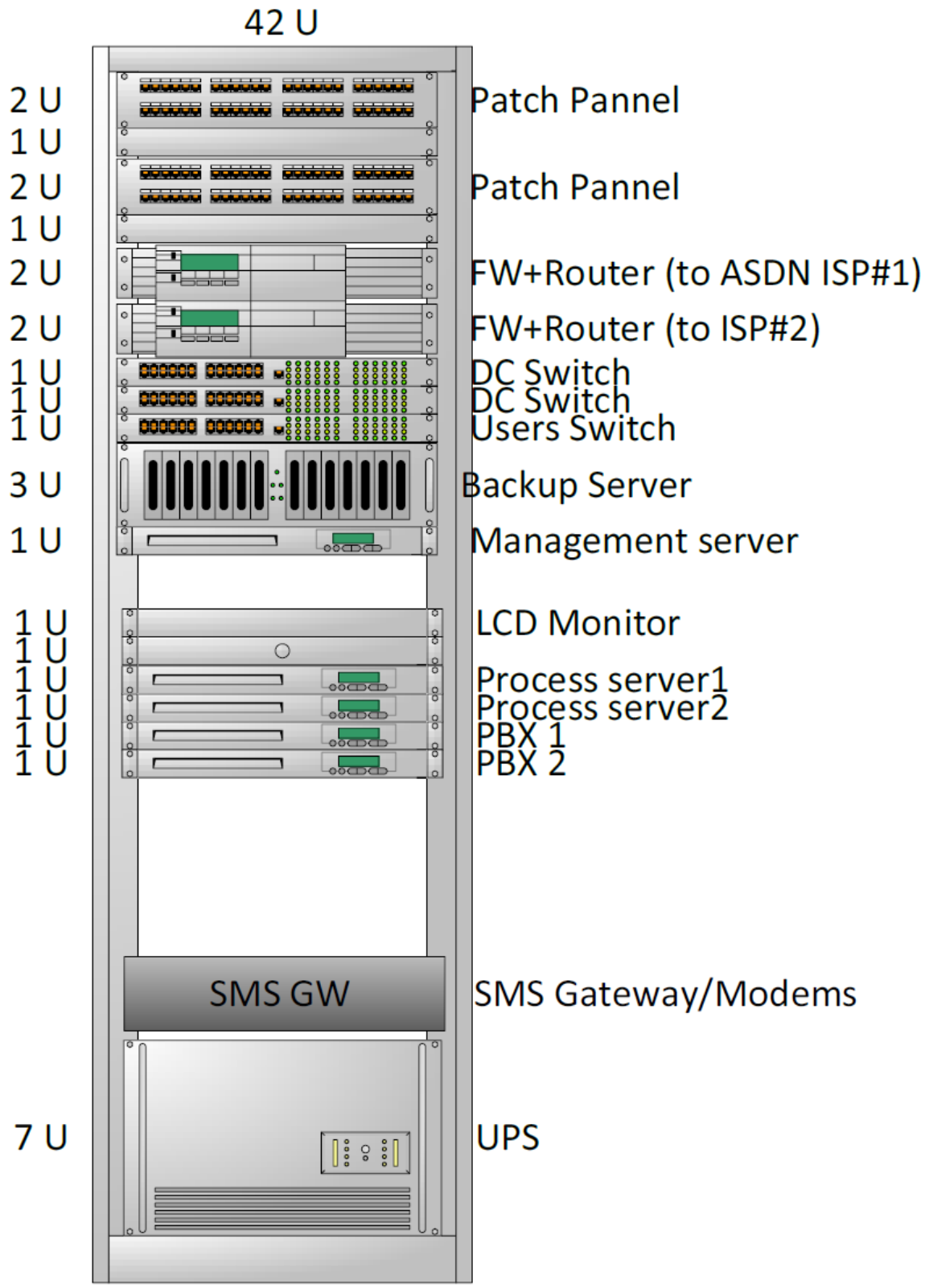
System Hardware

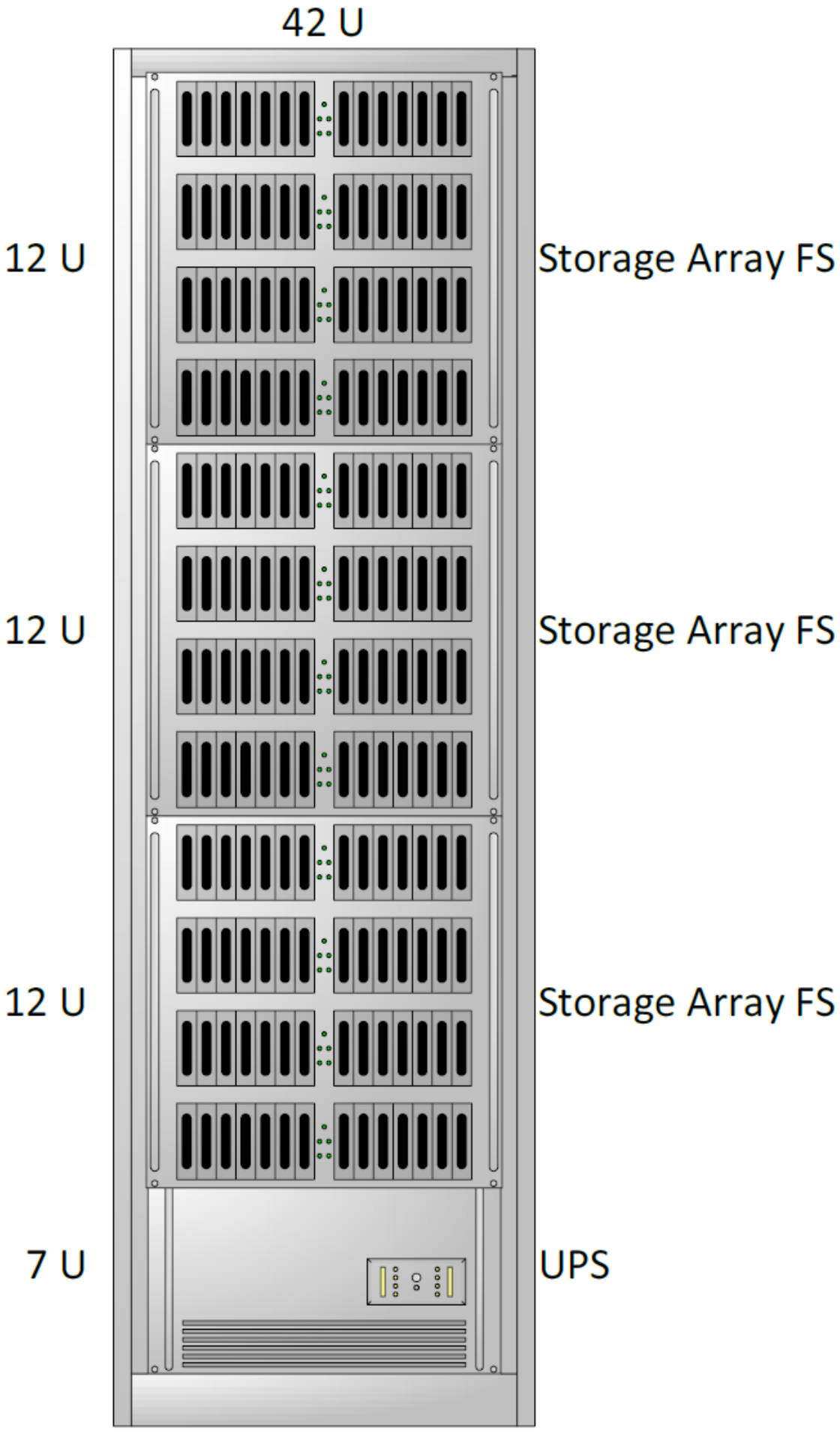
To fully support the system infrastructure, the following hardware is required:

- Two units of 42U cabinet
- Networking hardware
- 10TB of storage
- 5 standard servers
- UPS
- Cellular modems and SIM cards

The system hardware scheme is shown in Figure 11.

Figure 11: Pegasus Hardware




42 U
12 U
Storage Array FS
12 U
Storage Array FS
12 U
Storage Array FS
7 U
UPS

System Setup and Training

We are responsible for the system setup and training before its hand-over to the customer.

System Prerequisites

Successful installation of the Pegasus system requires the following preparations of the servers' room:

- Sufficient room to contain two 42U racks cabinet, 5x5x2.5m (LxWxH)
- Air conditioned (18°C) room
- Access restriction
- Routing from end-point terminals to servers room
- Reliable cellular network reception (at least -95 dBm)
- 2 x Electrical outlets (20A) per rack
- 2 x Symmetric ATM lines from different ISP's. Each line with a bandwidth of 10MB containing 8 external static IP addresses:
    - ISP #1: Fiber optic-based network
    - ISP #2: Ethernet category-7 cable-based network

  The mission-critical system requires two parallel networks to ensure system resilience and downtime is kept to an absolute minimum.
- 2 x E1 PRI connections, each contains 10 extensions (two different service providers is recommended)
- 2 x anonymous SIM cards for each local Mobile Network Operator
- 3rd party services registration as required

System Setup

- The solution will be deployed at the customer site by we personnel
- Deployment duration usually requires 10-15 working weeks
- Operating environment prerequisites must be met
- System setup includes hardware and software installation, and in addition integration to local environment and systems
- Support and adaptations to the different local device firmware versions

Training

Upon system installation, we personnel will conduct full training sessions. Training can take place onsite or in any other location required by the customer, including we headquarters. Training session includes the following:

- Basic system usage
- System architecture
- Advanced system usage and roles

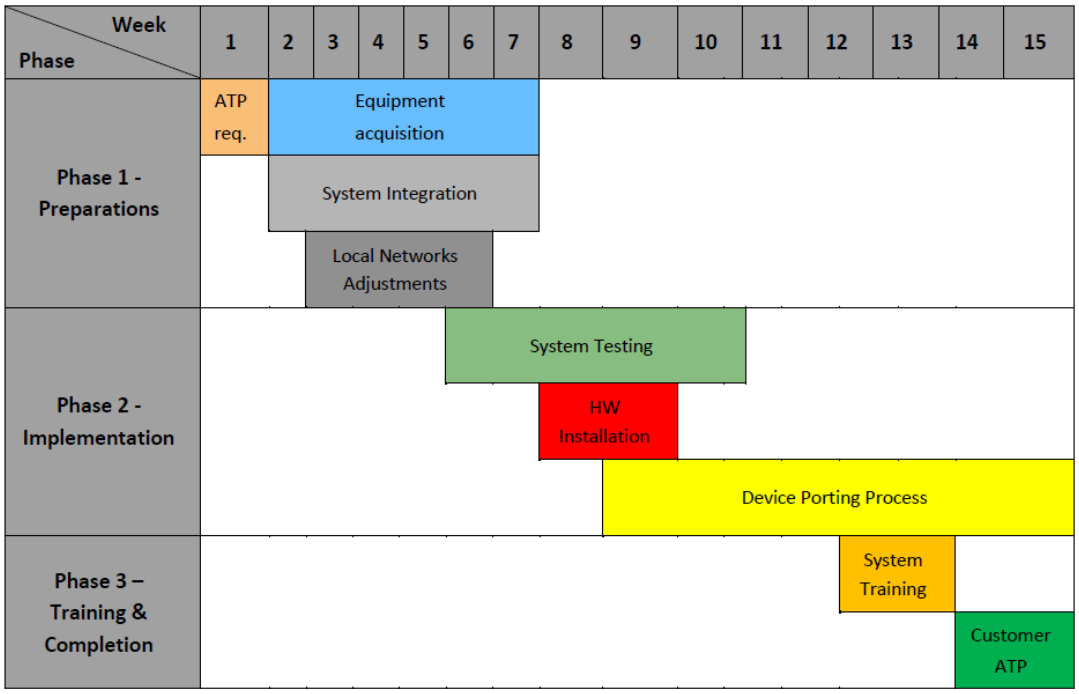
- Real-world simulation exercises

The recommended number of attendees is with respect to the number of installed operator consoles.

High Level Deployment Plan

The process of adapting, installing and testing the system in a new customer site in listed in Table 3.

Table 3: Pegasus Deployment Plan



Phase 1 – Preparations:

- Requirements for an Acceptance Test Procedure (ATP) are defined together with the customer
- Hardware and software acquisition and customization to answer customer requirements and needs
- When required, the Pegasus system is integrated with local infrastructures and systems
- System adaptations to the local mobile networks

Phase 2 – Implementation:

- System testing
- Hardware installation
- System adaptations to local device firmware versions

Phase 3 – Training and Completion:

- Detailed system training, real-life scenarios practicing and simulation
- Customer ATP as defined during phase 1

System Acceptance Test (SAT)

We have gained substantial experience in installing and implementing the Pegasus system. The following acceptance test plan verifies that the system works as required and validates that the correct functionality has been delivered. It describes the scope of the work to be performed and the approach taken to execute the proper tests to validate that the system functions as mutually agreed with the customer.

The tests are divided into 3 stages:

- Functionality tests
- Network and providers tests
- Customer tailor specific tests

An official system hand-over from we to the customer is done once the system has been deployed, tested and demonstrated.

Maintenance, Support and Upgrades

We provides, as default, one year of maintenance, support and upgrades services. These services include:

Maintenance and Support

We provides maintenance services and three-tier level support that includes:

- Tier-1: Standard system operations problems
  - Email and phone support
- Tier-2: Proactive resolving of technical problems
  - Dedicated engineers will inspect, examine and resolve common technical issues, putting their best efforts
  - Remote assistance using remote desktop software and a Virtual Private Network (VPN) where requested
- Tier-3: Bug fixing and system updates of substantial system malfunctions
- Phone support: In addition to the above mentioned, we provide phone and email support to any question and problem that is raised.

In addition, the customer will be able to add the following support:

- Planned or emergency onsite assistance
- Health monitoring system

Upgrades

We have releases major upgrades to the Pegasus system few times a year. Such upgrades usually include:

- New features
- New devices/operating system support
- Tailored features based on customer requirements
- Bugs fix