Airlines and airports present a unique security challenge. For the most part, they are open venues, located over a substantial area with large transient crowds of passengers. The security consideration is compounded by the fact that the manufacturer must also be mindful of operational considerations. Security is paramount but aircraft turnarounds time is important as well. Screening passengers is a necessary function, but when the passengers are standing in line, they aren’t shopping in duty-free.

The safety and security systems need to be multi-functional, protecting passengers, staff, equipment, food safety and the airline’s or airport’s brand. It must facilitate reporting, communications, crowd control, staff check-in and emergency management.

It must involve as many employees as possible and hopefully leverage the instinctive reporting capabilities that only human sensors can provide.

When an emergency occurs, the system must be able to ensure that the security networks do not crash and the security staff does not get inundated with information. The system must be designed to facilitate decision-making and turn vast amounts of data into actionable information.

Even during normal operations, the safety and security systems need to record every transaction so that the operators can take advantage of the audit trail and the lessons learned from prior incidents.

And to compound the challenge, the airport’s safety and security systems need to be priced at a lower cost per area covered than just about any other security application requirement.

In this white paper, we will discuss how a security and safety system based on smart mobile devices can meet the needs of airline security.
Background/Problems

The multifunctional considerations inherent in today’s air travel pose considerable security challenges. Airlines and airports must meet incredibly demanding criteria with regard to security, safety, and communications. Challenges include:

- Protecting passengers and employees
- Preventing terrorism
- Ensuring that staff and traveler traffic moves efficiently
- Integrating numerous subsystems
- Managing a wide variety of access authorizations

These challenges include knowing where the pilots, flight attendants, ground staff are located. They include monitoring perimeter areas, terminals, parking areas, aprons, baggage, cargo, shops, and other passenger facilities.

Airports and airlines increasingly use technology to innovate and help them meet their business goals. Airlines and airports must be very efficient and limit the number of false alarms. False alarms can slow things down when passengers and their bags need to be manually searched. Time-consuming security checks are more than just a nuisance; they can also impact airline schedules. Inefficient security can add to operating costs and can eat into corporate profits.

There are other examples as well. Crew work periods are tightly regulated. If the security system can fully integrate the access, emigration, dispatch, and time & attendance functions, it could possibly save each crew member one hour per flight cycle. This is, obviously, a huge efficiency improvement.

Another example is the possible reduction in the turn-around time of a plane from the current 90 min to closer to 60 min. This requires dynamic dispatch and staff management. If for instance, a crewmember started the check-in process but then was not found at the next step, there are two parallel considerations. One is to see what happened to the crewmember, but the other is to dispatch a replacement crew member immediately so that flight operations would not be impacted.

What is needed is a security system that will be able to monitor the entire airport, providing real-time situational awareness to the security staff. A security system that can be used across multiple terminals and airport operations requiring only a short set up time.

The purpose of this white paper is to describe an advanced, integrated approach to airport and airline security. One based on smart connected mobile devices that provide real-time situational awareness to airline and airport authorities.
Why systems based on smart mobile devices are ideal for airports and airlines

We generally think of security products as physical entities, e.g. Cameras, NVRs, Panels, Biometric Readers, some quite simple and some much more complex, built using sophisticated mechanical and/or electrical components. Maxxess has introduced a whole new class of security products that are smart connected security systems.

These are complex systems that combine hardware, sensors, data storage, microprocessors, software and connectivity in a myriad of ways.

Smart, connected security systems have three core elements: physical components, “smart” components and connectivity components. Smart components amplify the capabilities and value of the physical components, while connectivity amplifies the capabilities and value of the smart components and enables some of them to exist outside the physical product itself. The result is a unique cycle of value improvement.

Some of the unique features of our smart, connected security systems are:

1. **We facilitate the use of human sensors**

   Any security system should involve as many staff members as possible. It empowers your staff and makes them part of the overall security solution.

   People are the best sensors. They instinctively can sense that something is wrong. They can use smell, touch, taste, hearing and sight to arrive at a conclusion and then report that conclusion. They can call on their past experience to interpret what is going on. Together, the staff can form a human cloud of security that is much stronger than any physical sensor on the market.

   Each staff member is empowered “to see something; say something”.

2. **We provide a higher level of monitoring.**

   We monitor the system’s conditions, its external environment, and its operations and usage.

   Our dashboard allows the security manager to monitor all information related to staff reporting.

   The system analytics provide for quicker decision making. It can compare prior thermal mapping of crowd response to current data and integrate any new feedback from key staff members to the actual conditions that are occurring on the ground. All of this analysis is done in the cloud, aiding the decision makers from the storm of inputs they are receiving.
3. We control various system functions to better respond to changes in the environment, as well as to personalize the user experience.

A smart connected security system can leverage reporting, selective broadcasting, location information, automatic user identity, photographic transmittal, crowd sourcing and heat mapping.

These functions will relay any information to the correct department and have it analyzed instantly for quick decision making.

Our autonomous system operation can learn from the environment, adapt to users’ preferences and provide self-diagnostics and service.

Maxxess mobile systems can map or mirror any organizational structure, speeding up critical communications and getting any issue to the right person in the organization’s organization.

4. By moving the analytics to the cloud the system can be more robust than existing security systems.

The problem with many existing security and emergency management systems is that when a major incident occurs, those systems are rendered useless by the quantity of inquiries that hit the network. If the local network doesn’t crash then the decision makers will crash under the weight of the inputs. This can slow down or even paralyze the decision making process. Maxxess patented architecture uses structured messages and processes the storm of inputs in the cloud. All aggregating of responses or requests and associated analysis are done outside the local network. This ensures that decision making will be actionable and timely.

5. If an emergency occurs we provide two way, adaptive notification capability.

During normal day-to-day operation, the security system is handling a number of requests and reports. If an emergency occurs such as a natural disaster or a terrorist incursion, the system needs to operate bi-directionally and security staff needs the capability to direct people or groups of people appropriately. This adaptive response is necessary to minimize losses and optimize the evacuation process.

Digital systems can quickly analyze the situational awareness and share not only the awareness but the required response during important situations. This includes people and “things” like transportation vehicles and machinery that may have to be turned off after evacuating people.

The integration of text, photos and location alongside voice messages gives the organization flexibility in how their staff can communicate. A photo can often communicate much more
than voice or text. For example, if something needs to be repaired, employees can send a photo as part of the response to help describe the situation. Or, if there is a suspicious person, a staff member can send a photo to security and security can decide whether to broadcast it out to the rest of the staff.

6. These digital based, smart connected systems can provide “lessons learned” feature as a quick aid to the security department to enhance their decision making.

Maxxess new digital based systems store past security scenarios, including previous responses and outcomes.

With this feature, the system dramatically changes the security and disaster training paradigm. Training is now an active part of the response. It can be used to develop responses for different scenarios.

During training, or an actual emergency event, the system maintains a complete audit trail of every decision and every response to that decision. No information is ever lost.

The organization can also add pre-determined response scenarios including any rules, regulations or expectations that the organization might have for the particular type of incident being reported.

7. All of the above at a Lower cost

The cost/benefit analyses of the Maxxess cloud based, smart, connected security systems indicate that the operational efficiencies of this type of system, which are individually modest, but relatively easy to quantify, alone provide a positive financial return.

The incident-related benefits can provide extraordinarily high return in those circumstances when specific events occur – but there is no assurance how many incidents will occur within a specified period of time. These benefits, therefore, should be equated to those currently provided by insurance.

Since the new systems do not require a separate infrastructure, they require little or no capital investment on the part of the organization and only minimal service configuration. This new type of system can be added incrementally and coverage can be expanded to meet the organization’s operational needs at any time without any cost penalty.
Ambit- A new Maxxess solution to aviation security

Electronic communications have effectively replaced more tangible forms of communication. Phone conversations replaced direct discussions; e-mail then replaced phone conversations, as well as letters, memos, and many other written communications. Texts, IMs and tweets have replaced informal conversations; teleconferences and VoIP have replaced face-to-face meetings and remote desktops have replaced actual desktops. As the workforce has developed a more mobile character, communications in general have assumed a mobile aspect as well – some forms more successfully than others.

Can airports and airlines avail themselves of new electronic communications technology? Absolutely. While current communications techniques, do many things well, there are some functions that they don’t do well at all. These include:

- A shared awareness and perspective between the airport or airline and its mobile workforce of important situations.
- An ability to extend the airport or airline’s security reach beyond the bounds of a terminal or a group of terminals – dramatically increasing the coverage of the security system.
- The ability for mobile workers to request support and attention from the airport or the airline in a natural and efficient way.
- An effective means for the airport or airline to immediately determining the status of their workforce to enable rapid and accurate planning of actions.

The ambit smartphone based technology does all of the above, and more.
What is ambit?

ambit is the first and only service that allows an airport or airline to exchange timely and efficient messages directly with the personal devices of its employees through a proprietary, private, fully secure, closed communications channel. ambit is an essential tool, specifically designed to enable the airport or airline to communicate with its workforce both as individuals and as a coordinated group for appropriate action and support. ambit is compatible with all popular mobile devices and carrier networks and can operate on an international basis.

What does ambit do?

ambit takes full advantage of the power of both mobile smartphones [and other mobile Internet-connected devices such as tablets] and the Cloud to provide this service to the airport or airline. ambit can be customized to meet the specific needs of each airport or airline and its use can be driven by the airport or airline’s individual policies and operational requirements.

With ambit, the Security Director is in two way contact with every staff member, receiving reports from them and conversely, broadcasting to them (situational awareness, surveys, bulletins, etc.) over a private network.

Every staff member can communicate to the security office and “See something, say something.” The communications is structured, intuitively and does not require staff training.
The value of ambit:

The value of ambit is ultimately defined by the utility it provides. Each airport or airline will utilize ambit differently and therefore, will see a different value proposition for it. There are several common elements to ambit’s value for all airports, although the balance among these elements may vary. The major elements are:

- **Operational efficiencies**: individually, the benefits of capturing assigned tasks and their due dates with appropriate reminders; organizationally, timely knowledge of the status of the mobile workforce.

- **Enhanced decision-making**: the ability of the Security Director to make rapid, fact-based decisions and to implement consequent actions that involve the mobile workforce.

- **Emergency response**: the capability of the Security Director to respond to emergencies that affect the staff and the travelers – either as individuals or as a group– independent of the location of individual mobile workers.

- **Training**: the capability to run an exercise and have complete knowledge of who went where, when and optimize mustering or lock down or evacuation procedures.

- **Security / Operations**: Promotes a See Something: Say Something culture

It is more powerful than any traditional security system, no infrastructure expenses!

How does ambit work?

The ambit system consists of three principal components:

- **The System Console (or System Client)** enables the Security Director to manage and monitor the ambit service and to participate in message traffic.

- **The Message Server** is a Cloud-based, fully secure server and database that mediates all ambit message traffic, analyzes response messages and other pertinent data and archives all ambit messages.

- **The Mobile Client** enables the airport’s or airline’s employees to participate in the ambit service through their mobile devices.
The System Client resides at the designated security office and provides the system dashboard, message manager and analysis console. The System Client communicates with the Cloud-based Message Server via the Internet using a set of well-defined Application Programming Interfaces [APIs]. The System Client contains a wide range of management and analysis processes that support the ambit system. In addition, the software allows the airport or airline to develop their own tools, based on their particular needs. The System Client can be installed on existing computers, is compatible with most Web browsers and can be implemented in virtually any operating system environment.

The System Client presentation screens are designed to enable the designated security system operator to effectively monitor both a large population of staff that may require support from the airport or airline. This includes heat mapping of unusual activities.

The System Client is primarily intended to be a function directly associated with a command and control center, it can be supported on mobile devices for field or emergency operations.

Examples of some of the System Client screen available are shown below.
**Message Server**

The Message Server resides in the Cloud. It has two primary functions:

- To mediate all interactions between the System Client and the mobile network or networks that support individual Mobile Clients.
- To maintain and analyze the database of all ambit system message traffic.

The computational, communications and storage capabilities of the Message Server can be adjusted to meet the airport or airline’s needs, while the Cloud environment, which is designed to handle millions of pieces of data at one time, can easily accommodate the burst demands imposed on the ambit system during periods of substantially increased traffic, without burdening Airport or airline resources. This allows the airport or airline to respond in a timely manner to significant unplanned events.

Maxxess manages the Message Server to meet the capacity, availability and archival requirements of the airport or airline as part of the overall ambit service.

Additionally, each ambit system is self-contained and independent of all the other ambit systems. It is therefore not possible to share or access information via the message server on ambit systems operated by different customers.

**Mobile Client**

The Mobile Client resides on the mobile devices of the ambit users. Depending upon the requirements, the Mobile Client may be implemented either as a native app or as a Web app. The Web app has the advantage of being compatible with all mobile devices and operating systems using standard Web browsers and of not requiring any installation on the mobile device, but can have performance and functional constraints when compared to a native mobile app. Mobile Clients may use a mix of Web and native apps within a single ambit system.

The Mobile Client can be customized to meet the requirements of the airport or airline, but it is intended to provide a simple, intuitive, interface for the mobile user. An example of a generic ambit top-level interface is shown below.

Major ambit functionality is available to the mobile user with a single click in the menu.
Working with ambit

Registration

In order to be used with ambit, each mobile device must be registered with the ambit system. The System Client manages the registration process. Individual mobile users can register multiple mobile devices with ambit and use them interchangeably with the system. Registration provides privacy, authentication, and security, as well as the ability to collect and analyze data contained in messages sent by mobile devices.

Well-defined APIs that allow for extensive customization to meet individual airport or airline requirements, and connects all three components of the ambit system: the system client, the message server and the mobile client.

Dashboard

The status of the ambit system is summarized and monitored in the system dashboard as shown below:

Each organization can customize the dashboard to meet its unique requirements. The purpose of the dashboard is to provide a quick overview of the entire system during normal, low activity periods of operation and to monitor the evolution of incidents during periods of high activity. ambit can provide complete details for all activities summarized on the dashboard.
ambit Messages

*ambit* has been designed from the ground up as a closed, private messaging system allowing the airport or airline to easily maintain contact with its staff and if desired, its citizens. It is built around a Structured Message protocol that includes both message data and metadata for efficient archiving and analysis of all messages. Unlike most messaging systems, *ambit* is not a peer-to-peer system, but rather a system in which the organization is the originator or the recipient of all message traffic.

*ambit* supports one-to-many distribution of messages from the airport or the airline, but unlike any other messaging system, *ambit* effectively manages the many-to-one flow of messages from mobile users to the organization, letting the organization make rapid, informed decisions based upon both the aggregate response from the mobile users and the specific responses from individual users.

Survey

A key element of *ambit*s capability is the mobile response to an airport or an airline survey, such as a staff availability during a disaster. Like other messages, surveys are pushed from the Message Server to mobile devices separately from all other communications [e.g. IMs, texts, tweets, email] alerting the mobile user to the arrival of a survey message. An example of an *ambit* Survey message is shown below.

![Survey Message Example](image)

The structure of the Survey message is designed so the mobile user can respond with just two clicks, but it also permits the inclusion of additional information via the “More Information” section.

The combination of privacy, the *ambit* message structure, the mobile user interface design, and the message server analytic functions have demonstrated the ability to receive and analyze more than 90% of staff responses in less than five minutes – regardless of the size or location of the mobile users.
This provides the organization with a powerful tool for taking effective, informed, timely actions that reflect the intelligence and status of a widely distributed staff. The ambit survey has utility in response to unplanned incidents such as fires, natural disasters, exceptional weather or infectious disease outbreaks, but also has value for informing routine organizational operational decisions.

Shown below is the survey system flow and a representative survey summary display.
Monitor & Support

ambit’s Monitor and Support capabilities are initiated by a message sent from staff to organization. An example of a support request would be a major incident, from a major tarmac accident to a broken baggage carrier.

The Monitor function reflects a request by the staff member for enhanced attention from the airport or the airline. The Monitor message typically represents a security concern on the part of the staff member that can be escalated to a request for assistance. The actions of the organization in response to these messages will be dictated by its policy, but may include both direct and external [e.g. first-responder] support. The airport or the airline can provide updates on the status of support activity via the Monitor function, allowing the security staff to extend the reach of its security actions to all (or some) of its mobile users irrespective of their location.

Shown below is the monitor system flow and a representative Monitor summary display.

The Support function is an additional mobile-user-initiated message capability that allows individuals to provide unsolicited information to the organization regarding their environment. This information may be related to security, external events, or even routine operational issues such as terminal maintenance. Once again, the structure of the ambit system is designed to enhance the likelihood that mobile users will relay even low-level information to the organization.

While Support messages are typically expected to reflect the input of individual mobile users, there are situations in which the ensemble of Support messages from large numbers of mobile users can provide meaningful information [i.e. crowdsourcing]. As in the case of responses to Survey messages, the ambit message server will manage a burst of Support messages from the mobile workforce without burdening the communications, networking or computational resources of the organization.

The Support function, in a manner similar to the Monitor function, extends the observation and situational awareness of the Security Department using the inputs of the airport or airline’s employees.
Check-in (Time and Attendances)

The Check-in function permits the organization to maintain the real-time status of its entire distributed workforce. This status is valuable for routine operations such as assignment and dispatch of individuals, but it is critical also for establishing the configuration of the entire workforce for emergency responses to unplanned events.

*ambit* provides the necessary infrastructure to provide the information required for the organization to make critical staffing decisions, and the communication of the organization’s actions directly to its workforce.

Shown below is a representative Check-in summary display.
When ambit is used in conjunction with Maxxess’ eFusion security framework, *ambit* provides physical access control to airport or airline owned facilities without a separate credential and without any direct communication [e.g. NFC or BLE] with the access control hardware. This function is intended as an exceptional access activity, not routine access control.

Shown below is a representative access activity display.

The access function of ambit is an example of a functional capability resulting from the integration of *ambit* with another system – in this case eFusion. It is possible also to integrate *ambit* into other systems via the Event Relay function discussed below.

**Task**

Task allows the mobile user to store tasks that they may assign to their staff along with the expected due date. The system will alert the mobile user if the assigned task is not cleared by the due date.

Shown below is the flow chart for the task function and a representative task display.
Because of the highly unstructured nature of the environments in which the Support function may be required, ambit provides the ability to augment the written information in the message with an associated Media component [e.g. photograph from the field: a broken bridge, an accident at an intersection, graffiti]. Media will be archived and associated with the appropriate message traffic.

Event Relay

ambit includes an Event Relay capability which is the ability to forward ambit event information in real time from the Message Server to the organization’s systems that are external to the ambit system via well-defined APIs. An example would be a disaster that affects all airport or airline departments. These other systems can take subsequent action on these events with no additional interaction with the ambit system. In this context, an event is any activity that creates an ambit database entry including both organization generated and mobile-user-generated messages.

An example of the setup of a wide range of Event Relay items is shown below along with an example of the status of Event Relay activity available to the System Client.
Structured Messages

Structured Messages enable ambit to maintain a database of all message data and metadata, which can be used by the organization to assess and analyze the state of its staff either individually or as a group. Structured messages use pre-defined forms such as “yes” or “no” responses or a multiple-choice list of responses, to which the mobile user may reply. This allows the airport or airline’s security staff to quickly and easily assess a situation. Additionally, both outgoing messages, from the organization to its staff and incoming messages, from an individual or many individuals to the airport or airline, are archived and analyzed through a Globally Unique Identification number (GUID). This provides the organization with valuable audit information such as message origination time and location of the user.

The ambit system’s structured message protocol provides the following:

- Effective and efficient creation of database records with sufficient information to analyze messages receiving a large number of responses.
- Prioritization of responses by criteria associated with elements from the multiple-choice list contained in the original message.
- Aggregation of responses by list element choice, user classification, location of response, time of response, or any other characteristic contained in the message structure.
- Fast and convenient initiation of a message [response or independent message] by the mobile user; typically consisting of a selection from the multiple-choice list and a response confirmation.
- Clear segregation of independent messages initiated by the mobile user from the messages initiated by the security department through the system client and corresponding responses to those messages.

Message database

ambit maintains a record of all message traffic and supports both real-time and after-action analysis [for, e.g. training or forensic purposes]. This function is critical for scalability of ambit and for the extension of analytic capabilities over periods of potential interest.

Privacy

ambit ensures its service is private by requiring all devices utilized by its mobile users to be registered with the system and by requiring that all messages to mobile users originate at the organization’s offices.

Authentication

All ambit messages are authenticated because all messages to ambit mobile users originate at the organization while all ambit messages from mobile users must come from registered devices. ambit messages from the organization are pushed to mobile users via technology already available on all major mobile devices thus ensuring that these messages stand apart from any other communication traffic on the mobile device [e.g. text, IM, tweets, e-mail, phone mail] and receive immediate attention from the mobile user.
The private and authenticated character of the ambit message, along with the message structure itself, significantly enhances the timeliness and response efficiency to all ambit messages, but particularly, the response of large numbers of mobile users to Airport or airline Survey messages. The graphic below highlights the benefits with advantages of more than 100-to-1 compared to traditional communications techniques.

These benefits ensure that ambit remains robust even in environments of degraded mobile networks, directly translating into operational efficiencies for the airport or the airline.

**Security**

ambit messages are secured through encryption on all data in transit among the System Client, the Message server and the Mobile Client, as well as the closed and structured nature of the ambit system itself. Additional security features such as encryption of the system database and/or enhanced database replication and archiving techniques can be used to augment overall system security, if required.

**Message Analysis**

One of ambit’s unique capabilities is the provision of both real-time analysis of the state and context of the organization’s workforce, as well as forensic analysis of events documented in ambit message traffic. In addition to its operational benefits, ambit’s forensic analysis utility provides a powerful tool for the conduct and assessment of training activities for the workforce.

ambit’s correlation engine turns raw data into actionable information. Since all of the analysis is done in the cloud, the system only delivers high level decision information to the system console.

**Keeping the Storm in the Cloud**

The problem with many airport or airline security and emergency management systems is that when a major incident occurs, those systems are rendered useless by the quantity of inquiries that hit the organization’s network. If the local network doesn’t crash, then the decision makers will crash under the weight of the inputs. This can slow down or even paralyze the decision making process.

ambit’s patented architecture uses structured messages and processes to handle the storm of inputs during an incident. All aggregating of responses or requests and associated analysis are done outside the organization’s local network. This ensures that decision making will be actionable and timely.
Conclusions

This white paper describes an advanced, integrated approach to airport and airline security. One based on smart connected mobile devices that provide real-time situational awareness to airline and airport authorities.

ambit is an important, new element in an airport and airline security system that provides protection for large open venues and transient crowds of passengers. It can be used to identify security problems early and not allow those problems to escalate.

- A patented system that operates in the cloud and can be configured to meet the needs of any airport or airline.
- A security system that actually frees up passengers, minimizes impact on personnel throughput and can improve plane turnaround times.
- By using smart mobile devices, ambit allows an organization to get more of their staff to participate in the security process. It can harness the power of a worker's instinctive feeling that something is wrong.
- The unique characteristics of smart mobile devices complement other communications and mobility tools while taking direct advantage of the powerful devices the members of the mobile workforce already use.
- ambit is multi-functional. It can be used for day-to-day operations as well as for training and for emergency management response.
  - Real-time situational awareness
  - Includes knowing where the pilots, flight crew, ground staff are located at critical times.
  - Includes monitoring perimeter areas, terminals, parking areas, aprons, baggage, cargo, shops and other passenger facilities.
  - Thermal mapping limits the number of false alarms
  - Fully integrates the access, emigration, dispatch and time & attendance functions.
- It can adapt to your organizational structure, alerting the designated security officer and routing those alerts to any designated personnel in the various organizational areas.
- Can be used across multiple terminals and multiple airport operations.
- When an emergency occurs, ambit ensures that the security networks do not crash and the security staff does not get inundated with information.
- The system is designed to facilitate decision-making and turn vast amounts of data into actionable information.
- The system provides an audit trail that can be used to show "lessons learned" during any similar, future incident.

ambit is more than just "the cost of security". It is one of the few security systems where the organization can measure a Return on Investment (ROI).

The operational utility that ambit brings to the organization should provide an ever increasing level of security and an ever increasing positive Return on Investment.