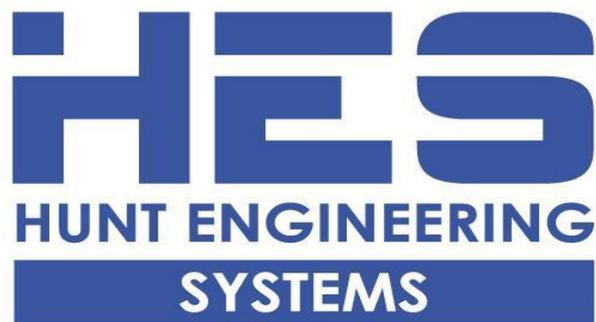


**MAX Visitor Management System**  
**A Cloud Solution for Prescreening Visitors And**  
**Issuing Visitor Passes and Badges**



**Hunt Engineering Systems, Inc.**  
**Orlando, FL**  
**sales@huntinc.com**  
**407-212-3005**

This information is being supplied to your organization for use by its employees. No further dissemination to other contractor firms or vendors is permitted without written authorization from Hunt Engineering Systems, Inc. This is copyrighted material and must be treated as company confidential.



## Table of Contents

<b>Mission Statement</b> .....	<b>1</b>
<b>Executive Summary</b> .....	<b>1</b>
NCIC and Other Watchlists .....	2
<b>Section 1 –Description of Products</b> .....	<b>3</b>
MAX .....	3
MobileMAX.....	4
Major Features .....	4
MAX ID Badge and Visitor Pass Process Flow .....	6
Step 1 - Request.....	6
Step 2 - Approve/Disapprove.....	6
Step 3 – Issue .....	6
Step 4 - Manage.....	6
Real-Life Scenario .....	7
Entering a Badge Request/Approval .....	7
Secondary Approval.....	7
Access Control Point .....	7
<b>Technical Description</b> .....	<b>8</b>
Enterprise Architecture .....	8
<b>Section 2 – Corporate Capabilities</b> .....	<b>9</b>
<b>Section 3 - Organization Information</b> .....	<b>10</b>
HES Points of Contact .....	10
DUNS and GSA Contract Numbers .....	10

## Mission Statement

Since the events of 9/11, Hunt Engineering Systems, Inc. (HES) has been focused on making facilities safer by positively identifying individuals that access facilities and preventing access to those who wish to harm people and assets.

Numerous mandates require military installations to perform NCIC checks on all individuals prior to allowing them to enter. This has imposed the need for more personnel and resources. This has also created challenges in getting these checks done in a timely manner.

HES has developed the MobileMAX as an easy and effective way to complete NCIC checks on all individuals. Checks are made on individuals when they preregister for access to the installation and again when they arrive at the installation. MobileMAX is an integral component of the MAX Visitor Management System.

## Executive Summary

This document presents information about our enterprise visitor management system known as the MAX. The name MAX refers to the MAX VMS or any of its related products. MAX is a full function total life-cycle visitor and badge management system. MAX manages visitor passes and badges from the moment of request, vetting, approval/disapproval, issue, and post issue management (track, recover, and dispose). MAX has been in use by various federal agencies including the US Military since 2002. MAX was conceived, designed, and built as a response to the events of 9/11.

We have divided this paper into the following 5 sections:

**Section 1 – Description of Products**

**Section 2 - Corporate Capabilities**

**Section 3 - Organization Information**

The MAX is an ideal solution for organizations that operate over an internal network (Intranet). An unlimited number of users in diverse geographic locations can use MAX installed in one central location to easily manage the entire lifecycle of visitor passes, badges, and ID cards. MAX has been deployed as an on-premise solution for the past 17 years, now HES has partnered with Oracle to provide MAX to military and federal government as a full function cloud solution in the Oracle FedRAMP compliant data center. Oracle provides a fault tolerant and self-healing enterprise database environment. MAX is the first cloud-based visitor management system that can offer automated real-time NCIC-III checks. The low-cost subscriptions and modular design make it ideal for both large and small military installations.

**Real-Time NCIC checks have been part of MAX since 2015. This capability is fully functional and in operation.**

MAX manages both visitor passes and badges collectively referred to as “credentials.” MAX has been

specifically designed around the concept that visitors and badged individuals will represent both US citizens as well as foreign visitors. HES has worked closely with cabinet and sub-cabinet level agencies to provide a powerful tool specifically tweaked for the management of foreign visitors. Lifecycle management includes:

- Register visit requests
- Prescreen/vet visitors and prospective badge holders
- Approve or Disapprove visit requests
- Issue visitor passes and badges
- Continue tracking passes, badges, and ID through entire lifecycle

## **NCIC and Other Watchlists**

The MAX may also include the MAX Watchlist Investigator. The MAX Watchlist Investigator is an interface between the MAX and multiple “watch lists” (sometimes referred to as “blacklists”). All prospective visitor pass holders and badge holders are seamlessly and transparently prescreened through the Watchlist Investigator prior to the issuance of any media. The Watchlist Investigator screens individuals through the following databases:

- NCIC – III (Triple-I)
- NCIC – Wants and Warrants
- State & Local – Warrants
- State & Local – Driver Registration
- State & Local – Vehicle Registration
- State & Local – Persons of Interest
- US Department of Commerce – Denied Persons List
- FBI – Most Wanted
- Palestinian Legislative Council
- Specially Designated Nationals
- Local Barrment Roster

MAX is designed to be modular which provides the ability to modify MAX to the exact requirements of the end user. The concept allows HES to provide the flexibility of a custom-built application at the price of an off- the-shelf (COTS) system. The modularity of MAX enables customers to use MAX as the central hub that integrates different systems built by other companies and government entities creating one seamless security solution.

Visitor identities are entered and/or validated by scanning a government issued ID. The scanning process is preferred by security specialists because it is faster, and more accurate than manual data entry. Higher quality scanners will also validate the authenticity of the credential while capturing the data. Each credential is subjected to white, infrared, and ultraviolet light. The behavior of graphic elements within the credential are compared to the correct template for the credential type. Credentials failing to match the template are flagged as fraudulent. Credentials that may be scanned include:

- Drivers' licenses
- Passports
- Military ID's
- Alien Registration Cards

## Section 1 –Description of Products

The following describes products and components produced by HES as well as its strategic partners. This explains how these components can be used together as a seamless solution to protect a facility from those who wish to do harm. The MAX Visitor Management System is referred to for the remainder of this document as MAX.

**Please note that all MAX functionality can be available to be licensed and used in other government systems.**

### **MAX**

MAX is a web-based portal that allows separate security-related components to work together as a single seamless security solution. MAX's primary goal is to significantly increase security and expedite throughput, while at the same time reducing staff loads and associated costs. Intrinsic in the MAX system is the fully integrated visitor management and ID badge management system that provides interactive, real time support to security and guard forces. Integrated computer software modules assist security personnel to rapidly assimilate visitor data to assist in making decisions about to whom to allow and to whom to deny access to critical facilities. MAX allows security personnel, sponsors, escorts, and other staff members to work together as a team to ensure that visitors and other badged personnel are properly accounted for during the time that they are on premises.

Security rules can vary widely based on who is visiting, their nationality, where the visit is to take place, the security classification of the visit, etc. The outdated manual processes make it difficult for security personnel to properly apply security policies when approving visitor passes, but MAX has been designed to apply complex security policies and to get it right each and every time.

The web-based MAX system provides for centralized and automated visitor and vehicle pass registration, ID badge control, and historical reporting. The MAX system is centralized, so it is capable of managing security from any computer on the organization's network. A single MAX installation may handle any number of facilities regardless of their global location.

One of the important features of MAX is that it permits authorized personnel to pre-enter expected visitors in the form of a "Visit Request." The request module allows personnel to enter and manage visitor pass and badge requests. The system can be configured to require zero-, one-, or two-level approvals before a visitor may be issued a visitor pass. Business rules regarding approvals may be based on multiple criteria such as: location of visit, citizenship of visitor, country issuing visitor's passport, sponsor's authority, etc.

MAX is very stable. Customers experience better than a 99.997% uptime. Some customers have enjoyed more than 9 continuous years of operation with 0% unplanned downtime. No data loss has ever been reported since MAX first went live in 2003.

## **MobileMAX**

The MobileMAX is a handheld scanner that is built on economical smart-phone or other mobile device platforms. Smart-phones are hardened by being placed inside cases designed for use by the security community. These hardened cases protect the phone from the hard use that is expected of security devices.

There are two configurations for MobileMAX units: Traditionally MobileMAX connects through a facility's own secure wireless network. Now with MAX being available on the Cloud MobileMAX is capable of connecting using FirstNET. A secure Nationwide network available to first responders and public safety professionals. This enables HES to offer both the MobileMAX devices and data connection as an add on to the annual subscription.

## **Major Features**

The following features help distinguish MAX from other solutions:

1. Browser based
2. Checks all prospective visitor pass holders and badge holders against NCIC, Published Terrorist Watchlists, Sex Offender Registries, Local Barrment Rosters, FBI's Most-Wanted, Online data sources, and any number of other lists uploaded locally
3. Shared Barred List
4. Unlimited users/licensed by site
5. Users are authenticated against LDAP, AKO, Active Directory, SiteMinder, etc.
6. Easy to use web-style forms
7. One-click upload of ID photos, signatures, and biometric data
8. Data entry by keyboard, document scans, file upload, and web service connectivity. Documents that may be scanned include driver's licenses, passports, other government issued ID cards
9. Unlimited number of badge designs based on affiliation, person type, US or Foreign National status
10. Manages both visitor passes and ID badges
11. Automates the total visitor pass/badge lifecycle process
12. Event Management
13. Turns all users into a single cohesive security team
14. Maintains historical list of all visitor passes and badges issued to each individual
15. No need to redundantly enter the same data as data values from previous badges and passes are automatically used when applicable
16. System may be accessed from any approved locations with internet access
17. User access is controlled by assigning roles (Role Based Access Control)
18. Uses an industry standard Oracle database
19. Annual subscription includes unlimited support, system wide updates, and RMF compliance

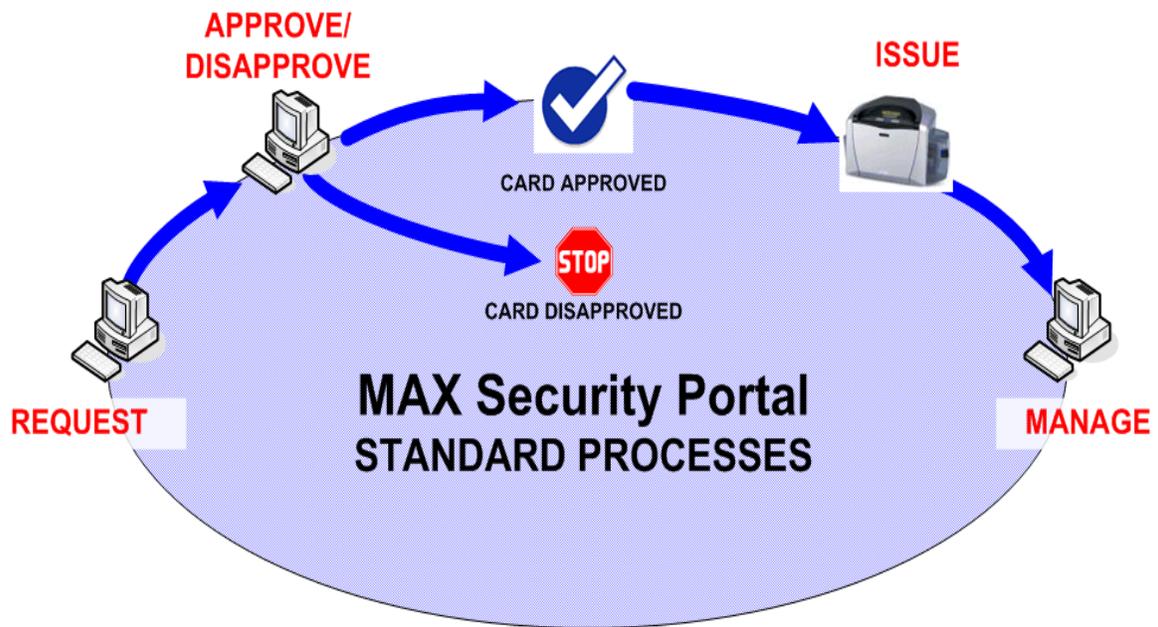


Figure 1 Typical MAX ID Badge and Visitor Pass Process Flow

## ***MAX ID Badge and Visitor Pass Process Flow***

MAX allows Security Personnel, Badge and Access Control Personnel, Contracting Officers, and Sponsors to work together as a team to ensure that badges and passes are properly accounted for during the entire life-cycle of the badge.

The typical process flow for creating an ID Badge or Visitor Pass is as follows:

### **Step 1 - Request**

[Optional] Someone with the proper authority inputs a request for an ID Badge or Visitor Pass to be issued. A simple web form is used for this that requires little or no training. All individuals entered will be screened through NCIC and other Watchlists.

### **Step 2 - Approve/Disapprove**

[Optional] An approval step can be implemented. This step requires that another user with the proper authority approves the issuance of the visitor passes and ID Badges. This step may be integrated with the Watchlist Investigator.

### **Step 3 – Issue**

ID Badges and Visitor Passes may be issued based on requests entered in step 1 and approved by step 2. Depending on local policies MAX may also allow ad hoc visitor passes to be issued without going through steps 1 and 2. Regardless of whether or not the person has been preregistered, another check against NCIC and other Watchlists will be conducted prior to issuing any visitor passes or badges. Each pass or badge can be issued on a variety of badge media including paper, PVC, card stock, etc.

### **Step 4 - Manage**

The badge and pass status may be monitored by those in authority. Such persons may be security force personnel, unit security managers, contracting officers, etc. In all cases, the data available to the user will be restricted by their access roles and affiliation with specific facility.

## ***Real-Life Scenario***

It is helpful to go through a real-life scenario to describe this process:

### **Entering a Badge Request/Approval**

**[1 to 2 minutes + 30 seconds per name]** – A sponsor is authorizing the visit of 2 US citizens. The identities are sent to the sponsor who then enters them into MAX. A header record is created that states the reason for the visit and the time of day that the visit will take place. Next the sponsor enters the names and driver license numbers of the visitors. Upon completion of the form the system will automatically send the names and identification information to the Watchlist Investigator. The Watchlist Investigator will flag any visitors that may fit anyone that has been placed on any of the watchlists. Any visitors that have not been flagged by the Watchlist Investigator are now “Conditionally Approved.”

Visitor information will auto-populate if they have visited any facility controlled by this MAX system in the past and their ID number (driver license number, passport number, etc.) is already on file. The sponsor may continue adding as many names to the request as desired.

### **Secondary Approval**

**[1 to 2 minutes per name]** – Depending on the authority level of the sponsor, location of the facility, the citizenship of the visitor, the results of the Watchlist Investigator, and/or other local policies, the visitor may require a secondary approval before a visit can be granted. When this is true the approver will receive an alert indicating that visitor approvals are required. An individual with approval authority may approve or disapprove the visit. An audit trail is created for any approval action. An alert is generated and sent to security administration if the approver is overriding a flag issued by the Watchlist Investigator.

### **Access Control Point**

**[1 to 3 minutes per visitor]** – The visitor first arrives at the Visitor Control Center (VCC). Guards can examine the government issued ID, CAC, or PIV used to preregister the visit and determine visually if the credential (driver license, passport, etc.) appears to belong to the bearer. Once this has been done, the guard will scan the credential to determine if it is genuine and if the visitor is expected. MAX will indicate to the guard if the visitor is to be allowed to enter the facility with or without an escort. MAX will also alert the guard if there is an issue that prevents the visitor from being allowed into the facility. Such issues may include but are not limited to:

- An NCIC or Watchlist check has flagged this individual
- Authenticity of the credential cannot be verified, or the credential has expired.
- The visitor does not have a valid visit request on file or is not expected at this time

# Technical Description

## *Enterprise Architecture*

The MAX was designed from the ground up to provide an Enterprise Solution to the problem of identifying and credentialing those who require access to a set of related facilities. HES has applied the standard business perspective to its MAX and related products. The four perspectives of MAX are as follows:

1. Business Perspective – MAX can be configured to conform to the business processes currently in use. The customer is **not** required to radically alter its business rules to conform to a rigid set of business rules imposed by MAX.
2. Application Perspective – MAX incorporates the necessary process flows between the distinct sets of functions. These steps are normally: Request, Approve, Issue, and Management.
3. Information Perspective – MAX enforces rules regarding data entry and data validation. This insures that entered data is usable, meaningful, and complete.
4. Technology Perspective – MAX uses enterprise grade operating systems, database engines, and application servers. The same technology employed at many of the top web content providers.

It is also important to remember that a cloud-based MAX is supported by HES. This alleviates Stress on an already overworked government IT staff. Cloud MAX will lower internal costs, enhance security, and enhance availability. Cloud MAX also relieves the DoD of the challenges of keeping everything compliant with prevailing accreditation, including time and cost.

## **Section 2 – Corporate Capabilities**

Hunt Engineering Systems, Inc. (HES) is the premier provider of web based, Enterprise class Visitor Management Systems (VMS) to the Federal Government, and the Fortune 500. HES is committed to improving security through innovations by providing its clients with the best visitor and credential management systems available today.

Founded in 1999, HES was profoundly affected and altered by the events of 9/11. Since 9/11, the Government has had a mission critical need to know who was visiting public facilities in order to maintain the freedom of access expected in the United States. HES responded with MAX, the industry leading Visitor Management System (VMS). MAX was adopted in the DoD and Civilian Agencies of the Federal Government – greatly improving security while speeding the visitor management process.

HES's expertise is in building large scale enterprise systems. These systems are used by organizations with thousands of users that may be spread over many different geographical locations. Typical customers use MAX in campus-like environments, including military bases, where the system must be accessible from many locations in many different buildings.

HES is focused on information technology products and services that enhance physical security for facilities and organizations as well as identity verification and background checks. The need for increased physical security and identity verification is a direct result of the current world strife.

In addition to the MAX product, HES systems engineers have also designed and built case management and intelligence processing systems to support large-scale criminal investigations and prosecutions. These provide for the storage, retrieval, and automatic distribution of investigative documents, crime reports, crime scene analyses, intelligence files, evidence collections, reports, criminal history analyses, and legal opinions; as well as images and graphics. The systems also support intelligence fusion through real-time access to national and criminal databases such as NCIC, and CJIS, as well as classified and published government data streams.

We have extensive experience in the generation of real-time security and intelligence products under crisis and time-critical conditions, as well as analytic and operational expertise in counter-narcotics, counter-terrorism, special operations, counterintelligence, threat assessment, risk assessment, arms proliferation, and organized crime.

## **Section 3 - Organization Information**

### ***HES Points of Contact***

#### Government Sales

Mr. Scott M. Hunt  
407-212-3005 Office  
850-819-2814 Mobile  
[scott.hunt@huntinc.com](mailto:scott.hunt@huntinc.com)

#### Corporate Address

7087 Grand National Drive  
Suite 100  
Orlando FL 32819  
407-212-3005 Main Office  
407-212-3006 FAX

### ***DUNS and GSA Contract Numbers***

DUNS number: 125212568 GSA  
Contract No: GS-35F-0307SCage  
Code: 3RBY2  
Fed ID#: 59-3710910