

factsheet

DIEBOLD'S LINX[®] PREDATOR ELITE GATEMASTER
An innovative solution for secure entry to government sites

- What Is It?** GateMaster is a complete, automated gate entry solution that includes gate access control, as well as a credentialing component for enrollment and authorization of personnel and visitors to military bases and other government campuses. The solution was created to process access requests quickly, efficiently and securely.
- Was It Developed by Diebold?** Like the core LINX system, GateMaster was developed by Diebold Security experts at the company's research and development facility in Moorpark, Calif.
- Who Should Use It?** GateMaster is the right solution when accurate identification and verification of all human entry is required at pre-determined access points before allowing site access. It can manage both foot and vehicle traffic while providing a fast and secure way for authorized personnel to be granted site access. When a person does not have the proper credential or that specific credential has been black listed, the system will not allow access and can be configured to trigger an alarm.
- GateMaster was developed to military specifications, but can be fully customized for use at a variety of government sites.
- How Does It Work?** GateMaster, a commercial off-the-shelf (COTS) solution, integrates a variety of access control, traffic regulation, barrier and credentialing devices to deliver secure, controlled entry to a variety of government sites. Once implemented, the GateMaster access control process includes:

Step 1A: Visitor Authorization

Like any credentialing process, visitor authorization begins with sponsorship. A sponsor uses a Web portal to provide information about the visitor. The sponsor can also preregister the visitor, providing information about when he/she will need access to the site and the period of time during which access should be granted. Once a visitor has been authorized, he/she uses a touch-screen, self-enrolling kiosk to provide additional detail and capture his/her image for a credential. The visitor then proceeds to the visitor control desk, where information is verified, the identity is compared to a black list of people who aren't permitted on the site, and other information is reviewed to approve or deny access. If access is approved, the visitor receives his/her visitor pass.

Step 1B: Personnel Authorization

Government personnel take their HSPD-12 compliant, government-issued credential to a visitor center to initiate the enrollment process. An enrollment operator reads the data on the credential and collects additional information, such as vehicle details. All information is then reviewed for approval or denial of access, as well as confirmation of permanent or temporary access. Optionally, personnel who are authorized for permanent access to the site can be issued an RFID tag that adheres to their vehicles for added security. Access parameters (including expiration date, if applicable) are confirmed in the system and uploaded to the credential.

Step 2: Approaching the Access Zone

If the person requesting access approaches in a vehicle, he/she will first encounter a vehicle loop that alerts an RFID reader that there is a vehicle to read. For those with an RFID tag, the reader provides initial verification of access authorization. The vehicle then encounters a lane pedestal reader, which includes both a bar code reader and a FIPS-compliant reader. The driver presents his/her personal credential to the appropriate reader. Next, the vehicle triggers the data capture loop. Here, an intelligent field controller confirms that the vehicle is past the point of data capture. If the system didn't capture all of the required information, the result is a failed access attempt.

If the person requesting access is a pedestrian, they enter a pedestrian lane. Bar code and FIPS-compliant readers are attached to a barrier such as a turnstile or gate. The person presents his/her credential or pass to the reader, and the system then makes a decision about access based on the information presented. Pedestrian traffic can also be managed manually using the system's IdentifyClient hand-held device.

The IdentifyClient hand-held device can be used to manually challenge a personal credential. It will display the outcome of the access request with a red or green screen that indicates the result of the access attempt and the corresponding person's dossier, which includes personal data and an image.

Step 3: Access Success or Failure

If the access attempt is successful, a traffic light displays a green arrow, confirming the vehicle and its passenger(s) are authorized to access the site. The vehicle is permitted to move past the gate arm for entry. If the access attempt fails, the vehicle remains outside of the gate arm, the traffic light displays a red "X" and a siren sounds. The site's security force then approaches the vehicle to confirm the validity of the failed attempt and take appropriate action. An additional layer of security is provided by the IdentifyClient hand-held device. The security force can use the IdentifyClient hand-held device to manually re-challenge the failed access request to determine if the request is invalid or the person did not present their credential correctly. This device is completely integrated with the rest of the system and displays credential detail, including photos, as well as a red or green screen that indicates the result of the access attempt.

Can It Be Used In Extreme Climates?

Because government implementations are located in a variety of geographies, GateMaster includes features that ensure its performance, even in the most extreme climate conditions. Customized enclosures can be used to protect various GateMaster devices from temperature extremes, as well as other climate-specific conditions, such as wind, rain, snow and ice.

GATEMASTER FACT SHEET/PAGE 4

Does It Meet Environmental Requirements? GateMaster was designed to meet stringent government requirements for protection of the environment. The components that are a part of the GateMaster solution were selected specifically to meet or exceed environmental specifications.

###

Contacts:

Media Relations

Rebekah Smith

+1 330 490-3773

rebekah.smith@diebold.com

Investor Relations

Christopher Bast

+1 330 490-6908

christopher.bast@diebold.com