Companies have traditionally relied on disparate security systems with different protocols and processes to manage physical and logical access. The cost and inefficiency of this approach, multiplied when considering visitors and those external to the organization, is dramatic. With an integrated platform, companies overcome the challenges of risk, scalability and accountability to protect assets – both virtual and real – from breaches, whether malicious or accidental.

The technology and business processes available today to achieve this integration – quickly, cost-effectively and without limits – give companies a way to assure identities and access for not only their own employees, but partners, as well.

**A Mission-Critical Challenge**

Exostar has an outstanding reputation for securely connecting the world’s largest aerospace and defense (A&D) manufacturers and their 40,000 supply chain partners. The leading provider of collaboration solutions, it manages an immense amount of intellectual property for its customers such as BAE Systems, The Boeing Company, Lockheed Martin Corp., Raytheon Co., Rolls-Royce, Northrop Grumman and the UK MoD.

Protecting assets, logical or physical, customer or corporate, is a top priority at Exostar’s Herndon, Va.-based headquarters. That’s why it relies on CertiPath and the larger Trust Bridge Community – the 4BF - to verify trustworthiness for physical and logical access for all employees and visitors.

CertiPath is the information-sharing bridge that connects that A&D partners with one another, and via the Federal Bridge to customers at the U.S. Dept. of Defense. As a member of the Four Bridges Forum (4BF), CertiPath is committed to promoting and educating the industry at large about the issues and solutions available for secure information sharing across organizational and geographical boundaries.

**The Future of Security: Physical and Logical Access in One**

Logical access control systems (LACS) have long been positioned as addressing the threat of a contractor who was terminated from continuing to access your systems through an account you provisioned; illegitimate access through legitimate means. This same risk exists for physical access control systems (PACS). An employee, who sets up a meeting with a customer for the following week and is subsequently terminated, may still choose to take the meeting and to disparage a company to its customer instead. Beyond the security improvement, the cost savings associated with a streamlined visitor check-in and check-out process add up quickly. Facility access logs are non-repudiable and when automatic, facility security audits simplified.

On any given day, 50 visitors come through the doors at Exostar. In the past, a visitor pass had to be issued for every single non-employee to enter the premises and the visitor required an escort to walk the building. Consultants needed to be set up on a workstation with security controls to prevent them from accessing proprietary information. A visiting engineer, for example,
might require access to a snapshot of production data, while a sales person would only require access to the Internet. If the individual was a frequent visitor, an Exostar laptop would be issued on a semi-permanent basis.

Exostar is rolling out the first commercially available integrated platform that manages visitors’ physical and logical access via their own organization’s issued credentials. CertiPath’s converged system eliminates the need to physically issue visitor passes and to be certain that each visitor is still employed and in good standing with their employer. The system extends the proven value of PKI-based security systems for managing and assuring logical access control to the challenges of managing and assuring physical access control.

**The system:**

- Leverages PIV, DoD CAC and PIV-I (draft) credentials issued by any valid issuer
- Utilizes FIPS-201 certified (or in process) components
- Allows customers to upgrade PACS without requiring replacement of the entire system
- Leverages commercially available products e.g Lenel (avoid/minimize custom solutions that are expensive to maintain)
- Leverages the US Federal Bridge to validate inter-agency trust (e.g., visitors)
- Delivers cost effective options to operate at one or multiple assurance levels (e.g., ‘controlled’ areas card only)

Today, visitors can use a single enterprise-issued smartcard badge with an embedded chip containing digital certificates to enter the building. That same badge is used by visitors to log on to their own workstation or laptop – a Federated One-Badge. The PACS implementation at Exostar is currently deployed at SP 800-116 maturity level 4 and contains three area profiles:

- **Controlled** – 1 factor of authentication is required (e.g. a smartcard that you have and can present). This level is available to Exostar employees only and is available only during business hours on the main floor.
- **Limited** – 2 factors of authentication are required (e.g. a smartcard and a PIN that demonstrates you know a secret). This level applies to visitors during business hours that have been sponsored by an Exostar employee and allows them to move about the main floor unescorted.
- **Exclusion** – 3 factors of authentication are required (e.g. a smartcard, a PIN and a biometric fingerprint read which represents something you “are”). This level is utilized after hours and for access to sensitive areas of the Exostar facility.

Exostar’s rollout of CertiPath’s converged system was so successful that it’s already making plans for phase 2 where attributes about visitor’s identities (such as citizenship) will be used to determine if access to a meeting in a conference room is appropriate. Information shared in meetings cannot be controlled via traditional LACS, so a meeting room PACS can be a useful solution. Much like the movement in A&D to have industry single sign-on for access to supply chain and collaborative applications, this federated PACS will create the same effect for visitors to facilities.

**Security Done and More**
The ability to conduct business every day with partners who are on the front lines of national security, knowing that physical and virtual access is truly controlled, puts Exostar at the forefront of an identity management revolution – where trust is the hallmark of transactions in all worlds.