

## CertiPath Launches Trusted PACS Service

### Expertise and Real-World Experience Accelerates ROI on Federated Identity Management Strategies

**HERNDON, Va. (Jan. 26, 2010)** — CertiPath introduces its [Trusted PACS™ Service](#), a much-needed solution for assessing, designing and deploying world-class identity and access control systems and processes. Combining deep industry expertise and a successful track record in managing implementations, the Trusted PACS Service helps resource-strapped organizations gain a faster path to the protection and operational efficiency provided by federated identity management.

Government agencies, transportation portals and many private sector companies are between a rock and hard place: required to meet stringent security mandates – such as HSPD-12 – but constrained by expertise, resources and time. When security solutions are implemented on a building-by-building basis, employees may be prevented from gaining access to do their jobs when entering a facility other than the one they report to regularly. The growing reliance on mobile workforces only increases risk and cost – creating armies of employees who don't have a single site where they work and who "hotel" at various employer sites. Add dozens of consultants, contractors and visitors who may need access for days or for months to complete a project, and the business case becomes apparent.

CertiPath's Trusted PACS Service overcomes this challenge so that organizations get robust, fraud-resistant identity credentials that meet the standards of an official accreditation process – quickly and cost-effectively. Using the Trusted PACS™ Maturity Model, CertiPath delivers actionable insight that supports the decision-making process. This model strategically assesses performance in key areas, including:

- Convergence between physical and logical access control systems
- Security of physical assets
- Identity federation for visitors
- Operational intelligence across the enterprise

With a federated PACS strategy in place that leverages public key infrastructure (PKI), companies lower the cost of issuing multiple badges and reduce the risk caused by lost credentials. Federated credentials for physical access control can also provide the foundation for extending access to partners, inclusive of supply chains, contractors and federal agencies – significantly streamlining data sharing, access control and permissions, based on the shared ability to recognize credentials issued by acceptable authorities.

**(more)**

## 2-2-2 CertiPath Introduces Trusted PACS

The Trusted PACS Service leverages CertiPath's experience in delivering identity management systems and credentials that meet the highest levels of assurance, as defined by FIPS 201 and the U.S. Dept. of Defense. The service provides solutions based on best-practices in building access solutions, managing identity credentials and PKI-based identity management solutions. CertiPath's industry leading expertise in these areas is drawn from the federal government as well as aerospace and defense giants including: BAE Systems, Boeing, EADS, Lockheed-Martin Company, Northrop-Grumman and Raytheon.

CertiPath's smart card and access control experts will:

- Assess current PACS and credential topology against the Trusted PACS™ Maturity Model
- Define a best-in-class identity and PACS strategy, including IT principles and alignment with business goals
- Establish a risk framework, including assurance levels and applications classification
- Provide gap analysis to address policy, governance, practices and technology concerns
- Recommend a sourcing strategy for technology

"Whether driven by federal mandates such as HSPD-12 or the need for more control and higher efficiencies, an integrated approach to managing physical access control for employees and partners just makes sense," said Jeff Nigriny, President of CertiPath. "We end the tug-of-war between building the ideal system and resource constraints – giving customers a clear, measured and testable approach to multi-building, multi-credential management."

### CertiPath Hosts Live PACS Demonstration

On February 2, [CertiPath](#) will co-host a live demonstration of multiple state-of-the-art, federated, [PKI-based](#) physical access control systems (PACS). The event is open to those responsible for physical security and information security in government organizations and companies that do business with government agencies.

Registration is required; to register please visit: <http://www.acteva.com/booking.cfm?bevoid=195470>. For more information about the event, contact Alison Kidd at [alison.kidd@certipath.com](mailto:alison.kidd@certipath.com) or (703) 793-7871.

###

### About CertiPath

CertiPath provides the aerospace and defense industry's only public key infrastructure (PKI)-based communications bridge where information can be shared widely, securely, effectively and affordably between partners, suppliers and customers – regardless of the size and scope of the supply chain.

CertiPath's solution tears down the burdensome and costly company, employee and program-centric approaches to identity assurance. Today, organizations in the U.S., U.K. and Europe including Boeing, BAE Systems, EADS, Lockheed Martin, Northrop-Grumman, Raytheon and the U.S. Federal Bridge (FBCA) are members of this fast-growing community. For more information, visit CertiPath on the web at <http://www.certipath.com>

### 3-3-3 CertiPath Introduces Trusted PACS

All product and company names herein may be trademarks of their registered owners.

**CertiPath Company Contact:**

Alison Kidd  
(703) 793-7871  
[Alison.kidd@certipath.com](mailto:Alison.kidd@certipath.com)

**Media Contact:**

Rachel Round  
(617) 969-9192  
[rround@corporateink.com](mailto:rround@corporateink.com)