



A Trusted Community Does Business – Around the Corner and Around the World

**A&D Pioneers Trust CertiPath for
Secure On-line Collaboration**

January 2010

Executive Summary

For aerospace and defense (A&D) companies, creating and delivering the solutions that protect nations around the world is no easy task. Competition is fierce and constant innovation is required for competitive advantage. And the growing threat of online attacks – whether designed to simply stop business from getting done or to steal intellectual property – makes the job more challenging.

Adding to the complexity is an expanding list of information security-related mandates from the stakeholders that matter most: the customer, in the form of government agencies, including defense and aviation agencies around the world.

In this environment, collaboration is critical, but it comes with the risk that mission-critical information could fall into the wrong hands. Overcoming this challenge is the sole purpose of the CertiPath trusted community, where employees, partners and customers around the world work together on-line, securely. The CertiPath trust fabric provides the highest level of assurance that the person sending the information – and the person receiving it – is who they claim to be.

Several industry giants, including **Boeing, Lockheed Martin, Northrop Grumman and Raytheon**, are certified members of the CertiPath trust fabric, and as a result, gain a secure and efficient means of sharing information across organizational and geographic boundaries.

“The advanced persistent threat is absolutely getting the attention of my executive team. As a member of the CertiPath community, we demonstrate that we’ve already got the infrastructure necessary to provide the highest levels of protection.”

— John Lyons, Senior Manager, Information Security and Chair, Boeing PKI Policy Authority

Business Challenge: Identity Assurance That Extends Beyond the Four Walls

As threats to electronic information become increasingly sophisticated and persistent, many A&D companies have invested in public-key infrastructure [PKI] based identity management solutions. These solutions are widely recognized as the most robust and secure for the protection of electronic information. While investments in creating these solutions are not inconsequential, the ability for employees around the world to collaborate with one another online justifies the cost.

The reality of business today, however, is that most companies rely on a highly extended and fragmented network of partners and suppliers to get the job done. Having an internal certificate authority (CA) only goes so far, according to **Jim Cisneros, deputy CIO of Boeing's Future Combat System program**. "It's like having a fax machine – it's great, but if no one else has one, it doesn't do you any good."

The challenge comes when companies seek to leverage internal CAs in partner and customer environments. The requirements for CAs that assert true identities are complex, rigorous and rigid, and each company has its own policies for mapping identities. As a result, even companies that have invested in CAs need to participate in a rigorous policy process for each and every partner and customer.

By becoming cross-certified to the CertiPath Bridge, these companies establish interoperable trusted identity credentials. CertiPath's model for "certified once, trusted everywhere" reduces the mapping and re-mapping from all involved to a single event. Within A&D, Boeing, Lockheed Martin, Northrop Grumman and Raytheon eliminated the need to recreate the certificate authorities used for working with partners.

Across A&D, these companies all work together and with common customers around the world. There's an immense need to collaborate and be able to share information electronically with a high degree of assurance.

"We have relationships with most other companies in our space – CertiPath is the hub that connects us all," says Cisneros. "It's a much better business model for us than if we had to do it 1-on-1 with all of our partners."

Agreeing to meet the standards and policies for identity assurance defined by CertiPath, each organization can now trust the assertions of others who have also been cross-certified. It immediately allows these companies to work with one another based on a common standard for rigorous and consistent identity authentication and management.

“By being a member of the CertiPath community, we are a demonstrated, trusted partner – verified by an independent 3rd-party,” adds **Michael Daley, Dir. Enterprise Security Solutions, Raytheon**. “Seeing our partners as Certipath members is very important to us, as it means that they have demonstrated operational excellence in their identity management and security practices.”

No longer needing to rely on shared service providers for 3rd-party credentials makes business sense as well.

CertiPath’s credentialing policies are designed to position members at the forefront of security in the supply chain (and create competitive advantage for themselves in the near term), with a system compliant with industry best practices.

“We eliminate the annual recurring costs of buying certificates and the costs related to managing them for thousands of employees – it’s a compelling business case in terms of millions in savings.”

—John Lyons, Senior Manager, Information Security and Chair, Boeing PKI Policy Authority

Authorization and access is based on two critical identities – the asset (be it a piece of data or a physical location) must be uniquely identified, as well as the requesting entity. The asset is evaluated against access rules that allow or deny a requesting entity. Only with these pieces of information can an access decision be made. Typical attributes about the entity that an asset owner wants to “know” before providing access include:

- Organization affiliation
- Business unit affiliation
- Job title and/or Job Role
- Citizenship

In CertiPath-enabled environments, digital identities include the typical attributes, and most importantly, what is most relevant to the supply chain – a person’s role and their organizational affiliation.

Cost-Effective, Scalable, and Secure Identity Assurance

The business case for federated identity management using digital credentials can best be described with a typical A&D scenario. A&D programs have very large supply chains with thousands of employees across the company and partners, who must all meet strict criteria in order to work on any given program.

Boeing’s Future Combat System is one model for tearing down the old way of managing identity management across the supply chain. As the lead contractor on the Future Combat System, Boeing found the need for collaborative tools as never before, and an immense amount of uncontrolled information. The combination requires that Boeing take all necessary measures to protect that information.

In the past, the prime contractor for a program would provision accounts for every individual at each partner in the IT systems that supported the program. When a partner wanted to gain access to that IT system, the employee would access the site, respond to an authentication challenge and be granted or denied access accordingly.

While this model correctly gives the prime control over access (i.e. the authorization decision), there are four major challenges:

1. The prime acts as the source of authority for the identity of all members of its supply chain, although they know much less about the individuals than their actual employer.
2. A trust relationship between the prime and its partners already exists via the contract that was executed in support of the specific program. Partners' employees would have been authenticated once – when they logged into his/her network at their desktop, prior to requesting access to the remote system, so the prime's authentication step is redundant.
3. The prime provisions a separate account for each person in the program's systems. Should an individual forget his/her password or require an update to any personal attributes, the prime must spend its own resources to service this request.
4. If something changes in the individual's status with his/her employer for whatever reason, the prime is dependent on the partner's organization to remember to update the prime so that access revocation can occur. This last point is one of largest IT security risks impacting the supply chain today.

CertiPath's solutions for cross-certified, interoperable credentials provide organizations with the ability to solve these issues. When combined with a single strong credential that is leveraged with all partners, members immediately eliminate the inherent risk of today's password-based approach for authentication. Boeing's Cisneros finds immense value in CertiPath's ability to shut access down instantly. "We have to take all measures necessary to protect information. With CertiPath, if you leave the company you are shut off immediately – our customers and partners really like this."

CertiPath's solutions for cross-certified, interoperable credentials provide organizations with the ability to solve these issues. When combined with a single strong credential that is leveraged with all partners, members immediately eliminate the inherent risk of today's password-based approach for authentication. Boeing's Cisneros finds immense value in CertiPath's ability to shut access down instantly. "We have to take all measures necessary to protect information. With CertiPath, if you leave the company you are shut off immediately – our customers and partners really like this."

For Lockheed Martin, the ability to extend the credentials to more than 90,000 suppliers has been a critical asset in keeping programs, including – the Joint Strike Fighter (JSF) – moving.

The global supply chain that supports the JSF is a totally new concept in which the aircraft is built in multiple sections around the world and as repairs or new parts are needed the aircraft itself sends messages about what is required back to the supply chain, via the U.S. Dept. of Defense.

Well before the JSF program, Lockheed Martin made significant investments in the infrastructure to support state-of-the art identity management. With JSF and other globally managed programs, Lockheed Martin optimizes this infrastructure. With a common credential, workers are able to come up to speed faster – and ultimately contribute to the programs much more quickly.

With Exostar, a CertiPath 3rd-party Certified Credential Provider, Lockheed Martin no longer issues credentials on behalf of suppliers, and with no loss of confidence. “We have bad guys attempting to gain access to IP and data on a daily basis,” says **Greg Roecker, Industry Alignment Manager of Lockheed Martin**. “Knowing who is on our network with high degree of certainty is extremely important to us.”

Eliminating the redundancy, inefficiency and risk of the old model delivers a cost-effective and highly scalable solution for managing and ensuring that information is exchanged only with those authorized to access it. **Keith Ward, Director of Enterprise Identity Management Solutions for Northrop Grumman** sees “tens of millions of dollars saved over 2 to 3 years.”

Winning Ways: Meeting the Customer Where They Are

In July 2008, the U.S. Dept. of Defense (DoD) CIO, John Grimes, issued memorandum 8520.2 which allowed the DoD to trust PKIs (Public Key Infrastructure) run by organizations external to them given that they met a number of criteria. CertiPath and its members meet these criteria and to date, only CertiPath customers have achieved PKI interoperability with the US DoD via their CertiPath cross-certification.

For members of the CertiPath community, this recognition delivered immediate and powerful competitive advantage. At the time, comments from **Jeff Brown, Chief Information Security Officer of Raytheon**, reflected the impact of DoD’s validation both on the investments made, and the industry’s overall mission. “This policy recognizes the maturity of our efforts – and the efforts of the whole CertiPath community – to deploy PKI-based security solutions that merit the DoD’s confidence,” said Brown. “With this shared foundation of trust, we can speed the efforts of the real mission – building national defense systems that protect against the evolving threats to our customers around the world.”

For Lockheed Martin’s Roecker, the Grimes memo gave his team the evidence needed to demonstrate internally the value of the company’s investment in cross-certification. “When the Grimes memo came out in July 2008, we got in the queue for interoperability testing right away and have made tremendous progress – it was much faster with CertiPath than if we had done it ourselves.”

Northrop Grumman is an early adopter of the solution and was one of the first to have credentials in place in accordance with the DoD policy. Northrop relies on the CertiPath solution to enable a wide range of communications channels, including e-mail, and a Web portal for supplier on-boarding for conducting business with customers including the U.S. Air Force. Like many others in the industry, the company is moving beyond user name and password to more robust solutions such as smart cards or USB-based credentials for systems that deal with sensitive information.

In a competitive industry, where the ability to demonstrate compliance with requirements and mandates is an absolute must, these companies and other CertiPath members are well-positioned to meet customer needs, even as requirements evolve. "It all comes down to secure collaboration with our customers, the U.S. Dept. of Defense and Federal Agencies – we can't do business without it," says **Russell Koste, Identity and Access Manager at Northrop Grumman.**

More recently, in May 2009, Robert Lentz, CISO and Deputy Assistant Secretary of Defense for the DoD, testified to Congress that A&D companies must balance the need to protect intellectual property while demonstrating willingness and ability to meet contractual requirements from government customers for auditable, identity-based, secure flows of information. His remarks reinforced the role of interoperable identity credentials in mitigating the risks related to compliance, complexity, cost and IT that are inherent in large-scale, collaborative programs that span national jurisdictions.

In addition to the DoD, CertiPath members' identities are trusted to do business electronically with the U.S. General Services Administration, the U.K. Ministry of Defence and the Netherlands Ministry of Defence. "As the business of defense increasingly becomes a global one, there's a greater need for international cooperation and standards for identity assurance," says **Alison Dunstan, former CIO and Assistant Head Identity & Privilege Management of the UK Ministry of Defence.** "CertiPath members have demonstrated that they have the infrastructure, policies and are as auditable for similar credentials as we in the defence community adhere to."

One Card That Does It All

There's a growing call to action in identity management circles for an integrated approach to identity assurance. CertiPath is leading the definition of standards with its IceCAP initiative. IceCAP is designed to bridge the gap between physical and logical access, by applying the best aspects of transparency and governance enabled by the U.S. federal government's identity assurance standard, FIPS 201.

Ultimately, the solution will allow CertiPath members to issue a single identity card, where information and authorization for an individual's access to both physical operations and information systems is stored.

Lockheed Martin is one of the CertiPath members testing models for the integration of physical and logical access – a “one badge” approach. “We have a significant population located on government facilities, accessing government systems,” says Roecker of Lockheed Martin. “A single credential that gives them access to the base and to the systems is a valuable idea for us.”

Commercial Aerospace Moves to World-Class Identity Management

Boeing, along with others in the commercial aircraft space, is driving the expansion of requirements for broader and more robust identity management solutions. Boeing’s Lyons sees the value of the work his company has done on the defense side having compelling value on the commercial side.

The newest planes in the Boeing fleets will leverage CertiPath-certified PKI for interaction with gate landing systems, called GateLink. An airport-issued credential that is CertiPath compliant can then be used by gate agents and ramp workers for:

- Coordination of maintenance requirements
- Baggage handling procedures
- Gate management procedures

In the hangars, there’s a move to require airport airframe maintenance workers to sign for every action they take on a particular aircraft in the maintenance log of that aircraft. This manual process is being automated by Boeing and others. Boeing is advocating the use of CertiPath-certified PKI for this new automated process. An airport-issued credential that is CertiPath-compliant can then be used by that worker for:

- Physical access to the security identification display areas (SIDAs) housing the aircraft
- Logical access to the updates of software downloads for maintenance of the aircraft
- Signature on certified logs on actions taken for a particular aircraft

Business, Done

For CertiPath members, cross-certification creates trust – with partners and customers. And while trust in and of itself is intangible in the A&D industry, it is an asset with exponential value.

Whether doing business around the corner or around the globe, CertiPath offers a business proposition that delivers what companies need most today – secure, scalable and trustworthy identity assurance.

“CertiPath is the right choice for three simple reasons – lower costs, faster collaboration and cyber security.”

— Russell Koste,
Identity and Access Manager
Northrop Grumman

For more information, please contact:

Alison Kidd at alison.kidd@certipath.com or (703) 793-7871