



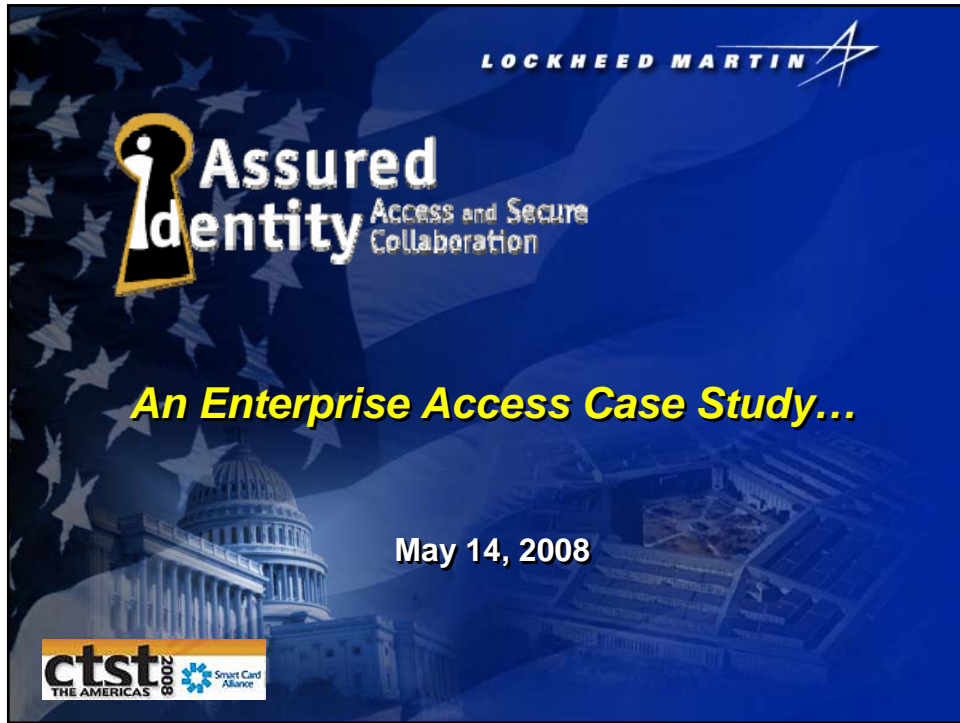
LOCKHEED MARTIN 


Assured Identity Access and Secure Collaboration

An Enterprise Access Case Study...

May 14, 2008

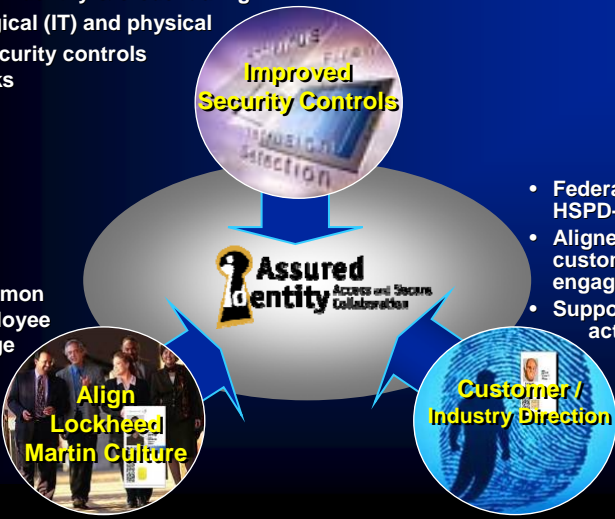
ctst 2008 THE AMERICAS 



LOCKHEED MARTIN 

Drivers

- Common identity & credentialing
- Both logical (IT) and physical
- Align security controls with risks




Improved Security Controls

Assured Identity Access and Secure Collaboration

Align Lockheed Martin Culture

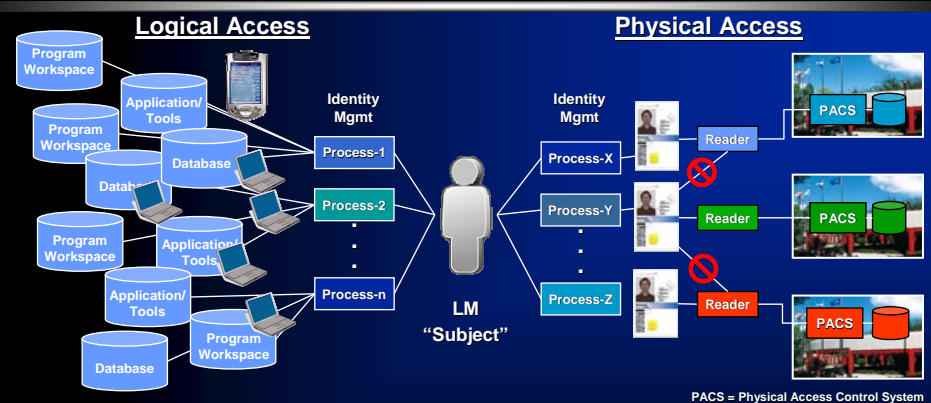
Customer / Industry Direction

- Common employee badge
- Federal ID standard: HSPD-12
- Aligned with LM customer engagements
- Support collaboration activities (TSCP)

 **Assured Identity** Access and Secure Collaboration

2

The Challenge

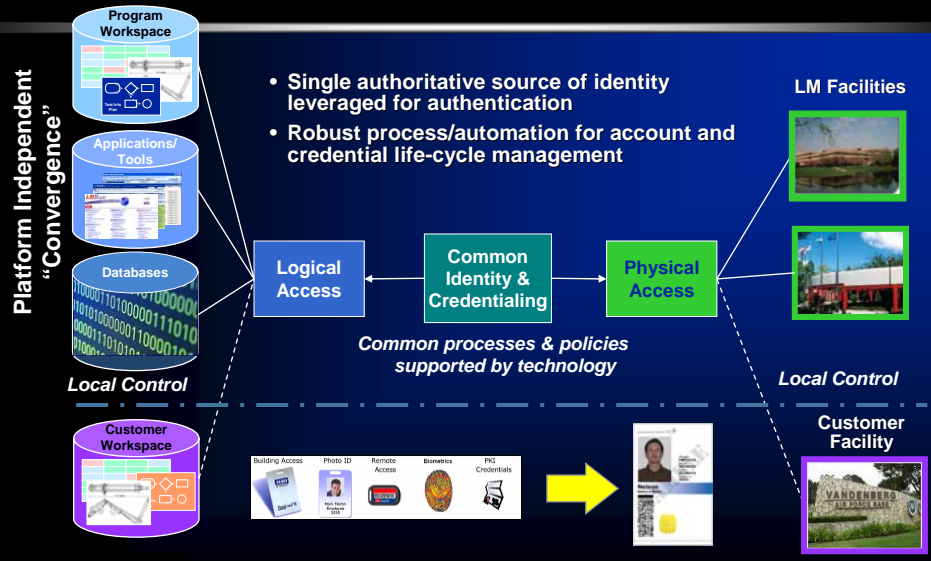


- Many, many processes for identity creation and access control
 - Typical LM employee has 10+ identities
 - Multiple types of credentials
 - Multiple identity data stores
- 100+ badging offices; unique processes
- Many employees require multiple badges
- Some badges used for logical access, ex. time & attendance



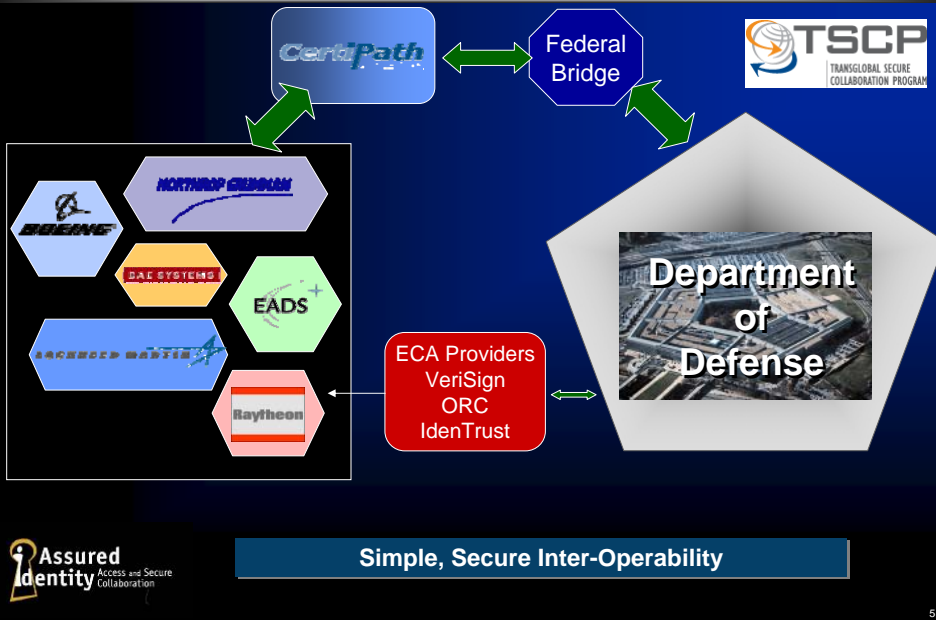
Complexities and inconsistencies lead to weaker controls

Program Vision

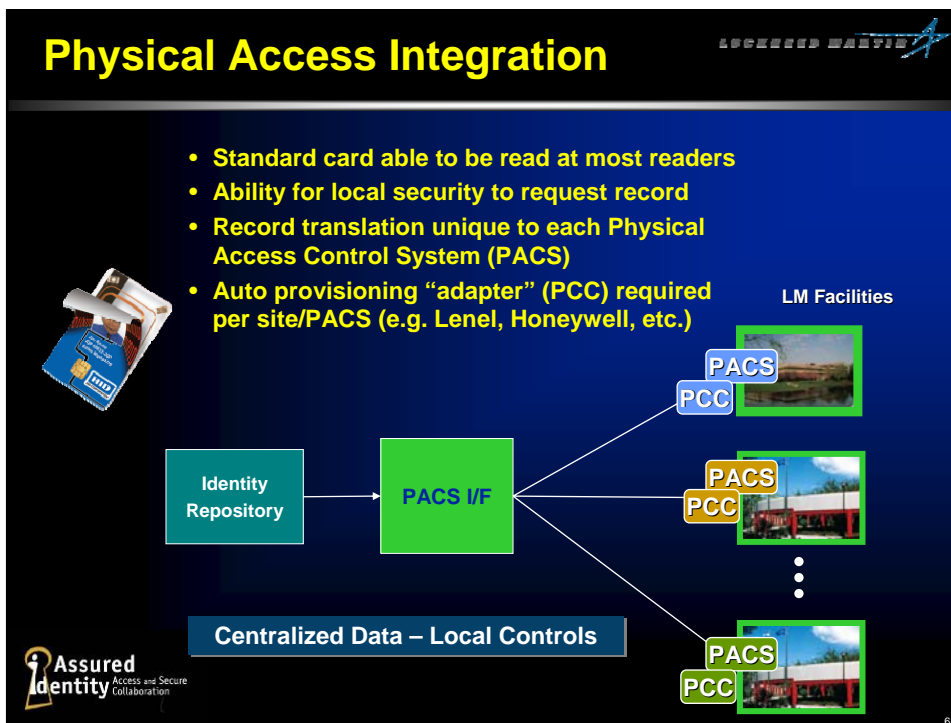


Reduced manual efforts, operational efficiencies, retired systems, increased data quality, stronger controls

Cross-Certification and Trust



Physical Access Integration



Lessons Learned



- Most benefit gained through Logical Access Integration efforts
- Smartcard provides some benefit (specifically for higher risk users/roles) but need Logical Access Integration to achieve full benefit
- Rapid deployment w/ enrollment drives business impact
- Significant business unit specific effort to realize full Physical Access Integration
- Must continue to work “Organizational Readiness” (awareness, change management, communications, training)



7

Summary



- Assured Identity, Access and Secure Collaboration extensive scope provides for stronger security controls and positions for industry alignment and secure collaboration
- It's all about access control!! Who is granted access based on what authoritative sources of information?

Reduced manual efforts, operational efficiencies, retired systems, increased data quality, stronger controls



8

