

e-Diagnostics Security Requirements Update

Anant Raman

anant.raman@intel.com 480.554.1538

October 19, 2001

INTERNATIONAL
SEMATECH

10/16/2001 3:43 PM j:\stndpres\template\IntST.ppt - 1

Agenda

- **Current Status**
- **Work in progress**
- **Challenges**
 - How to complete capability definition by end of Q4'01
 - How to make the current approaches scaleable to multiple suppliers and IC makers
- **Summary**

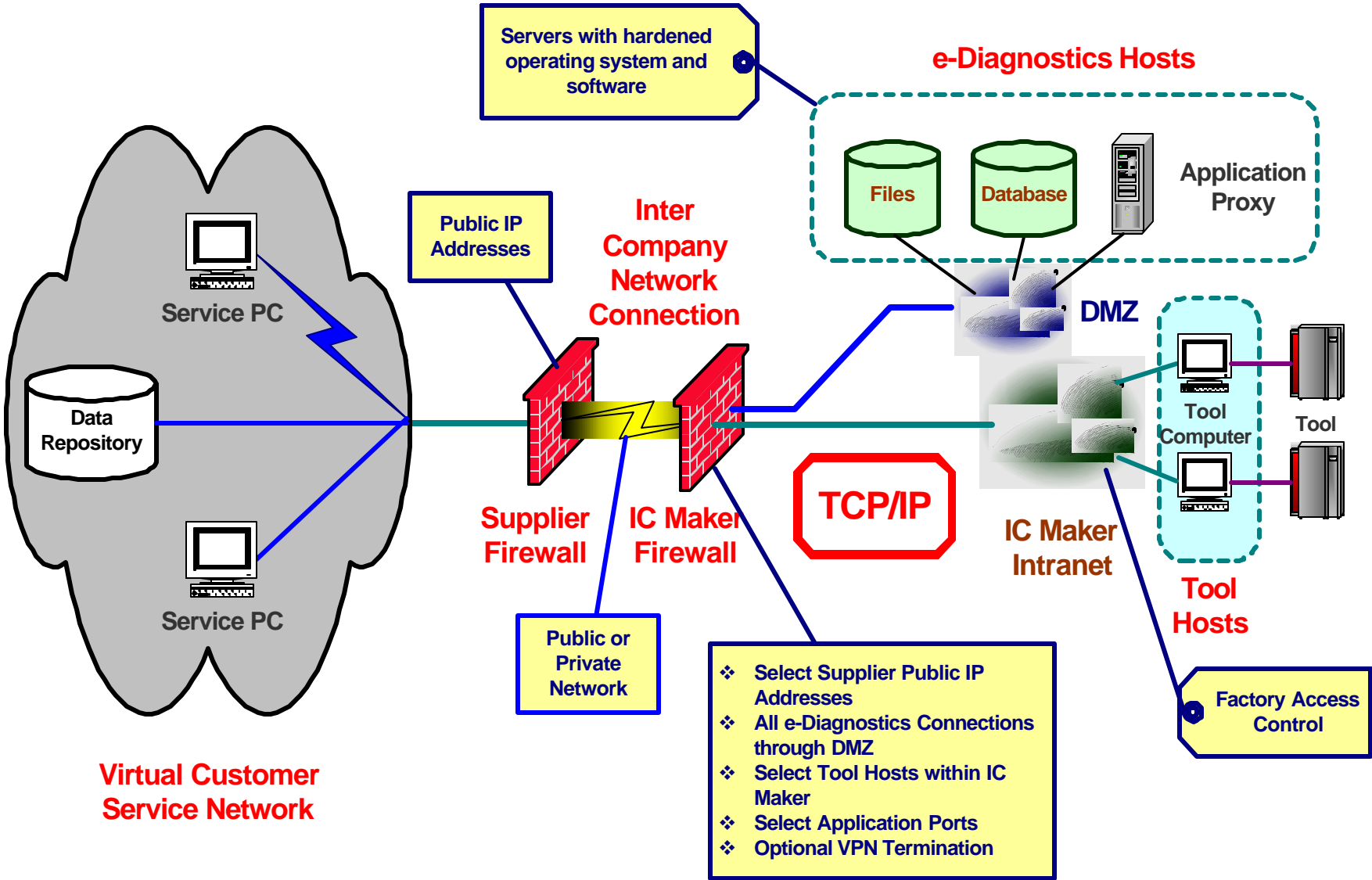
Current Status of Security Capability

e-Diagnostics Layer	Supplier	IC Maker	Supplier & IC Maker
Hardware-Connectivity	e-Diagnostics Firewall	e-Diagnostics Firewall	Inter Company Network
	Customer Service Network	e-Diagnostics DMZ	Network Security
	Service Computers	e-Diagnostics Servers	
	Data Repository	e-Diagnostics Factory Network	
	Firewall Access	Equipment computers	
Software-Logical	Web Browser	Authentication	Network Security
	Application Client (UI)	Authorization	
	Local User Login	Application Access	
		Equipment Data Access	
		Application Usage	
		Application Protocols	
		Data Classification	
		Data Confidentiality & Integrity	
		System Management & Infrastructure Services	

Red: Work in Progress

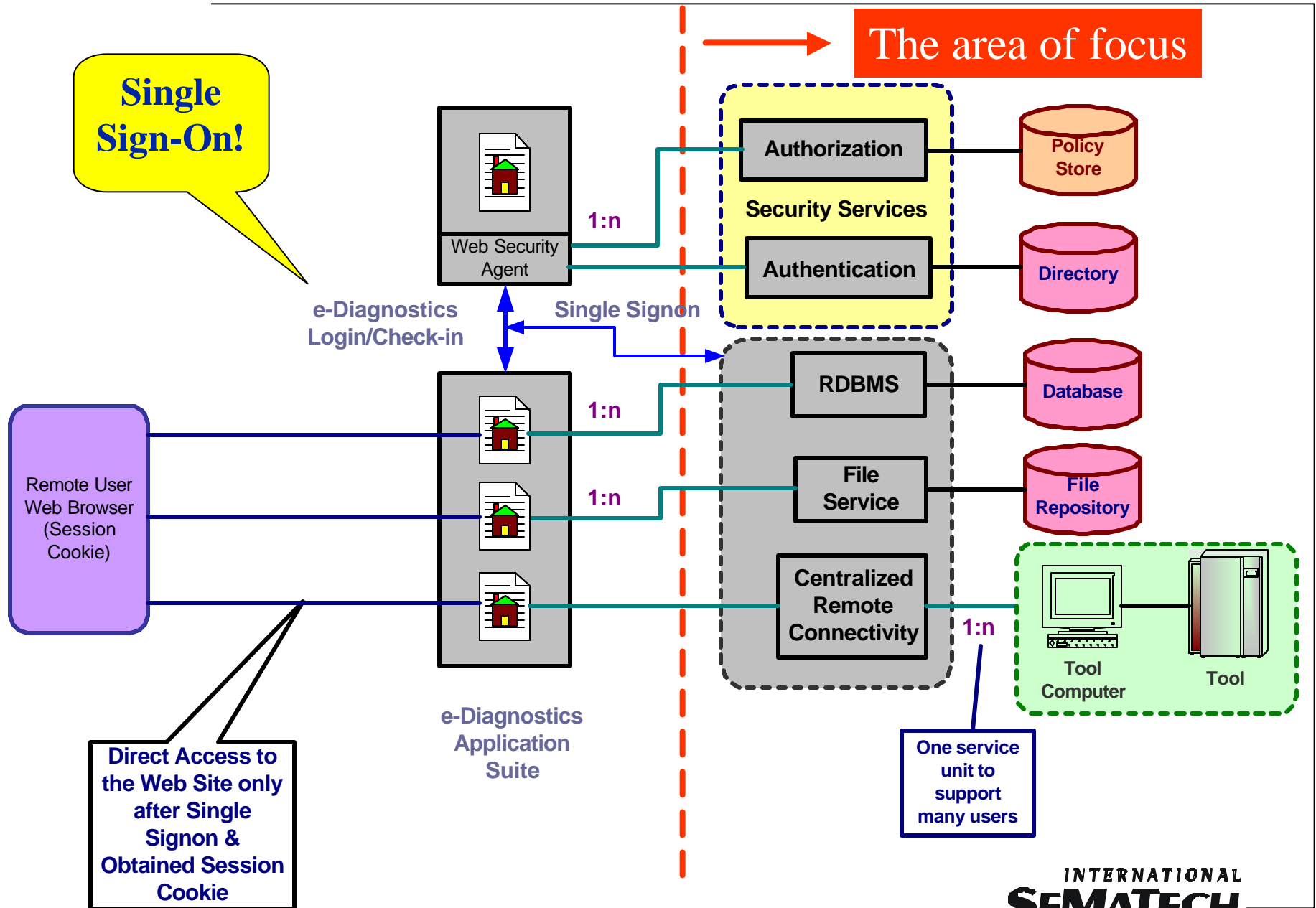
Plan is to complete all by end Q4'01

e-Diagnostics Hardware-Connectivity



We now need to harden the system!

Software-Logical Layer

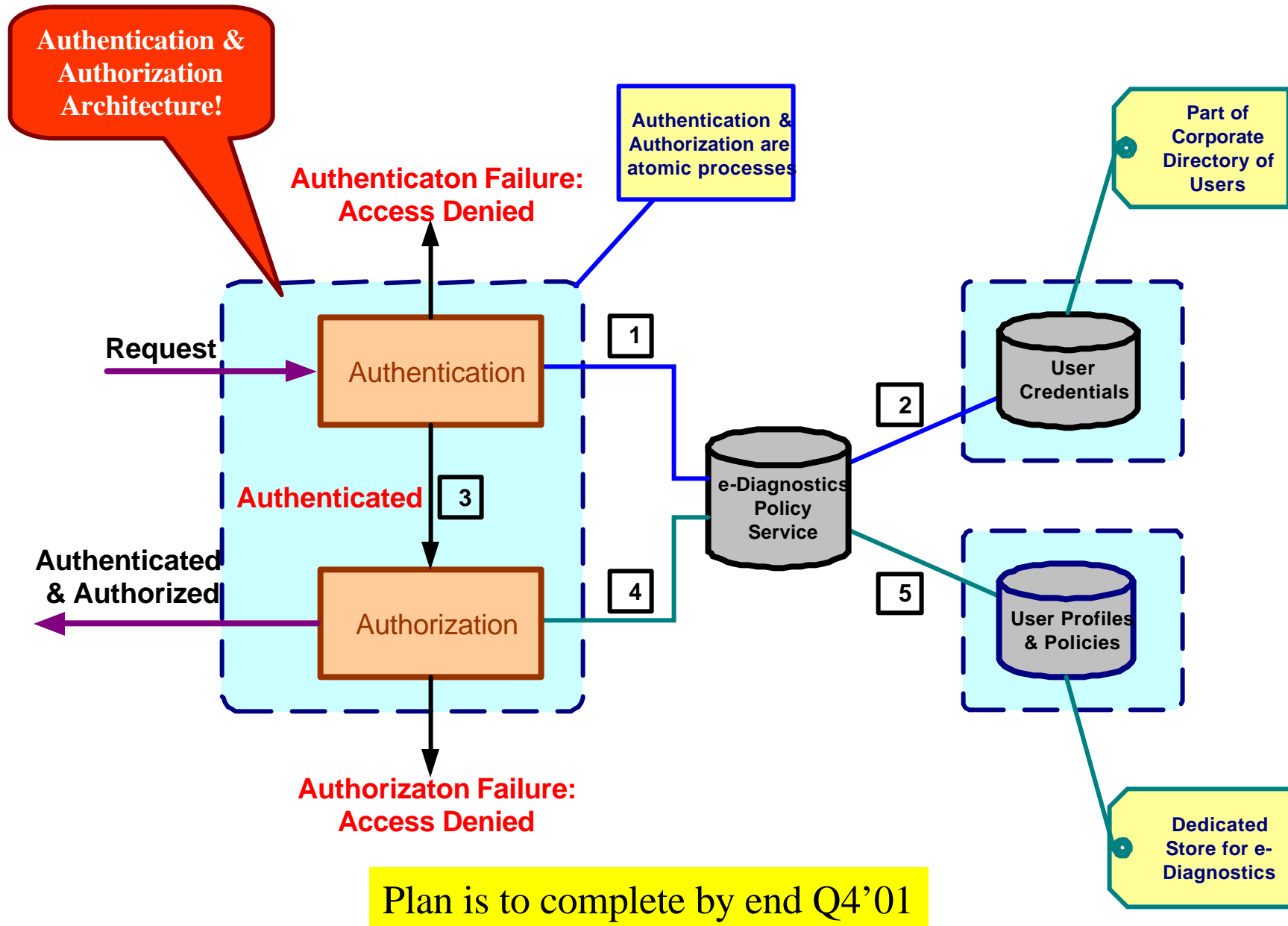


Software-Logical Layer

- **Work in progress in following areas:**
 - **Authentication:** Focus on PKI & Digital Certificates for all companies
 - **Authorization:** Modeling authorization for the various tasks within e-Diagnostics capability
 - **Application Access:** Single Sign-on with centralized security
 - **Equipment Data Access:** Driven by SEMI/DDA Task Force with focus on all activities except remote access
 - **Application Usage:** Secure remote access and application sharing with collaboration.

Plan is to complete all by end Q4'01

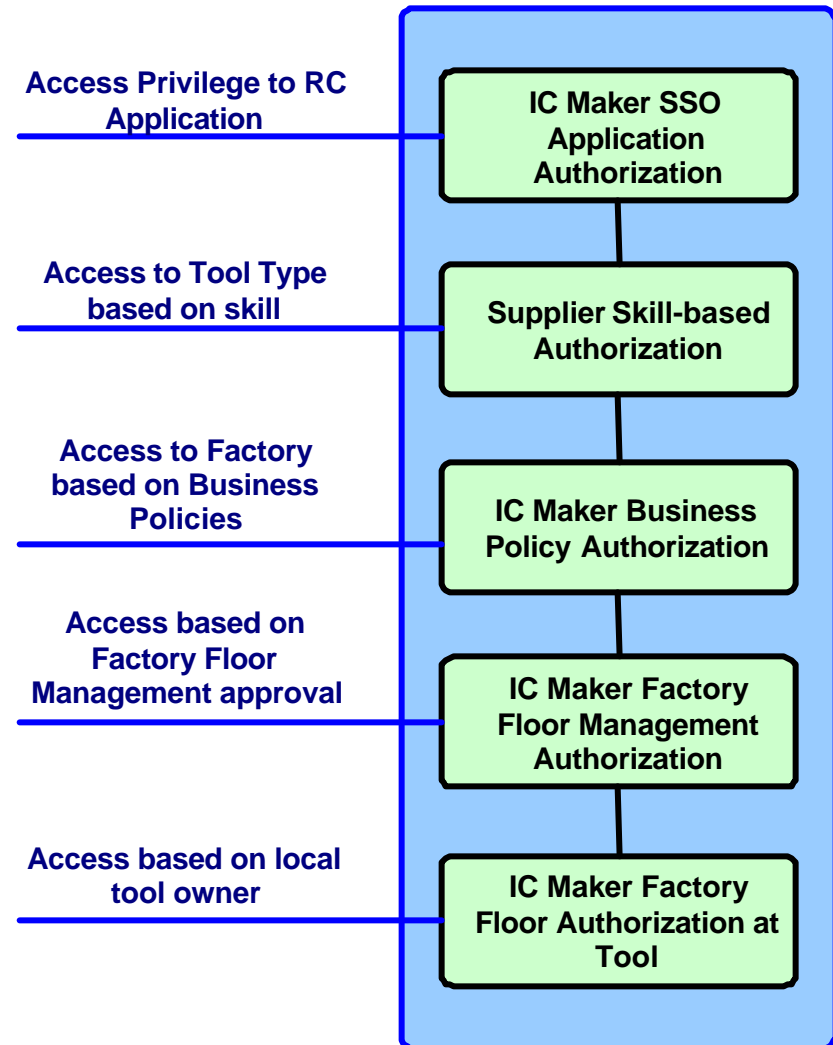
Most critical part of the security is...



Authorization Complexity

- **What authorization consists of:**
 - Various levels of IC Maker approval for task at hand
 - Supplier approval also required

Proper system design will resolve this complexity



Challenges for ISMT security team

- **Unified hardening procedures/guideline:**
 - Sharing of security procedures, virus solutions, software build parameters, etc. across all suppliers & IC makers
- **Unified PKI infrastructure – one certification authority**
 - Strive for one solution for all e-Diagnostics suppliers and IC makers; unlike RosettaNet (PIP)
- **Avoid custom security code/Don't re-invent!**
 - Use well-known, well-tested, standards-based and certified libraries and products.
 - Separate authentication & authorization from e-Diagnostics applications
 - **Third-party products provide best of breed in timely fashion**
 - **Different companies use different authentication & authorization products and methods providing an integration challenge.**

Summary

- **Hardware-Connectivity layer**
 - Essentially complete
- **Software-Logical layer**
 - Current focus for the team
- **Overall Security**
 - Lots of challenges. Need synergy here