

e-Diagnostics Security Update

Anant Raman (anant.raman@intel.com)

David Bloss (david.a.bloss@intel.com)

December 4, 2001

Agenda

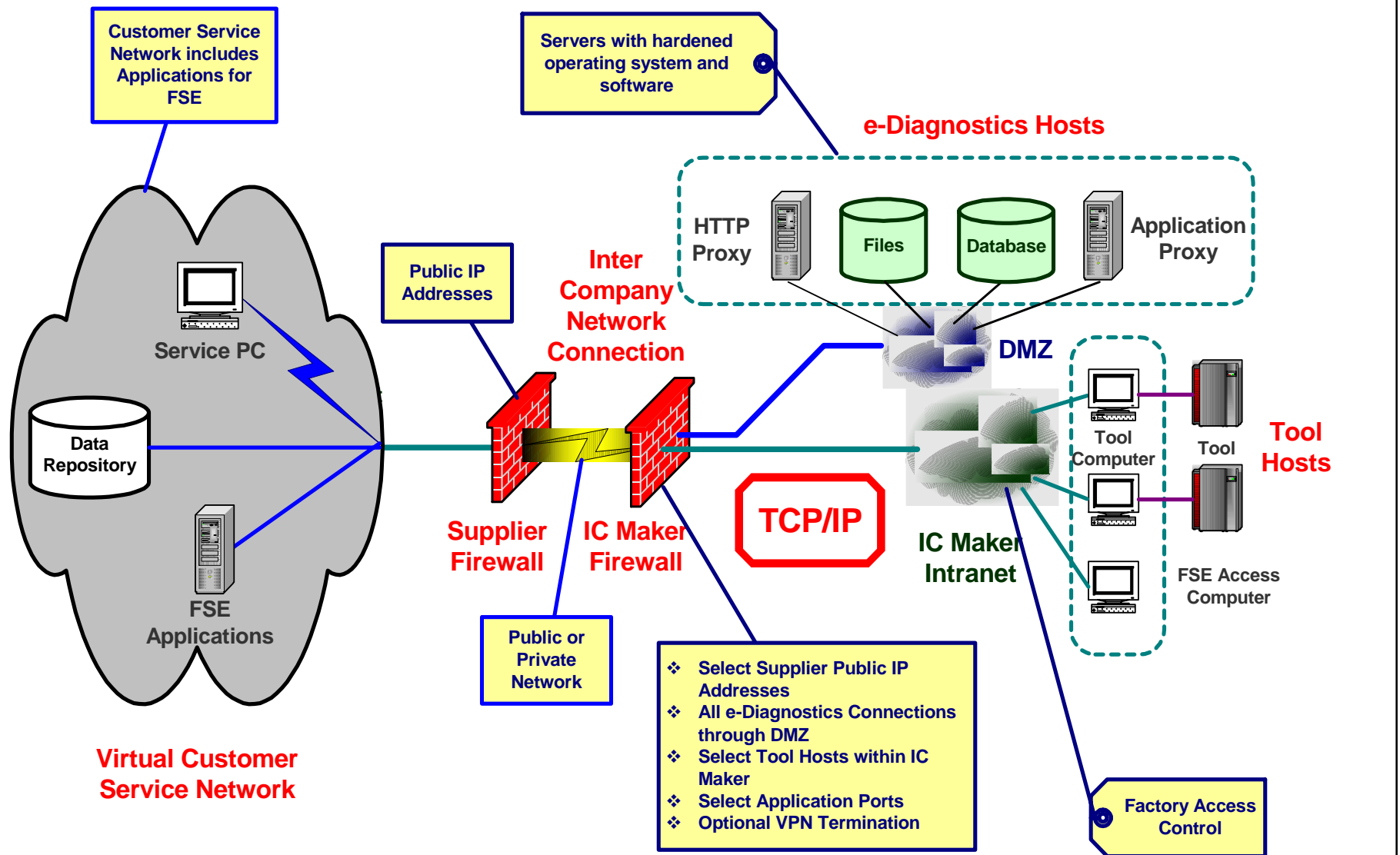
- **Current Status**
- **Work in progress**
- **Challenges**
 - How to complete capability definition by end of Q4'01
 - How to make the current approaches scaleable to multiple suppliers and IC makers
- **Summary**

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 Server Hardening	
	Data Repository	E-Diagnostics Factory Network	
	Firewall Access	Equipment Computer Hardening	
Software-Logical	Web Browser	Authentication	Network Security
	Application Client (UI)	Authorization	
	Local User Login	Application Signon	
	FSE Access Applications	Equipment Data Access	
		Application Usage	
		Application Protocols	
		Data Classification	
		Data Confidentiality & Integrity	
		System Management & Infrastructure Services	

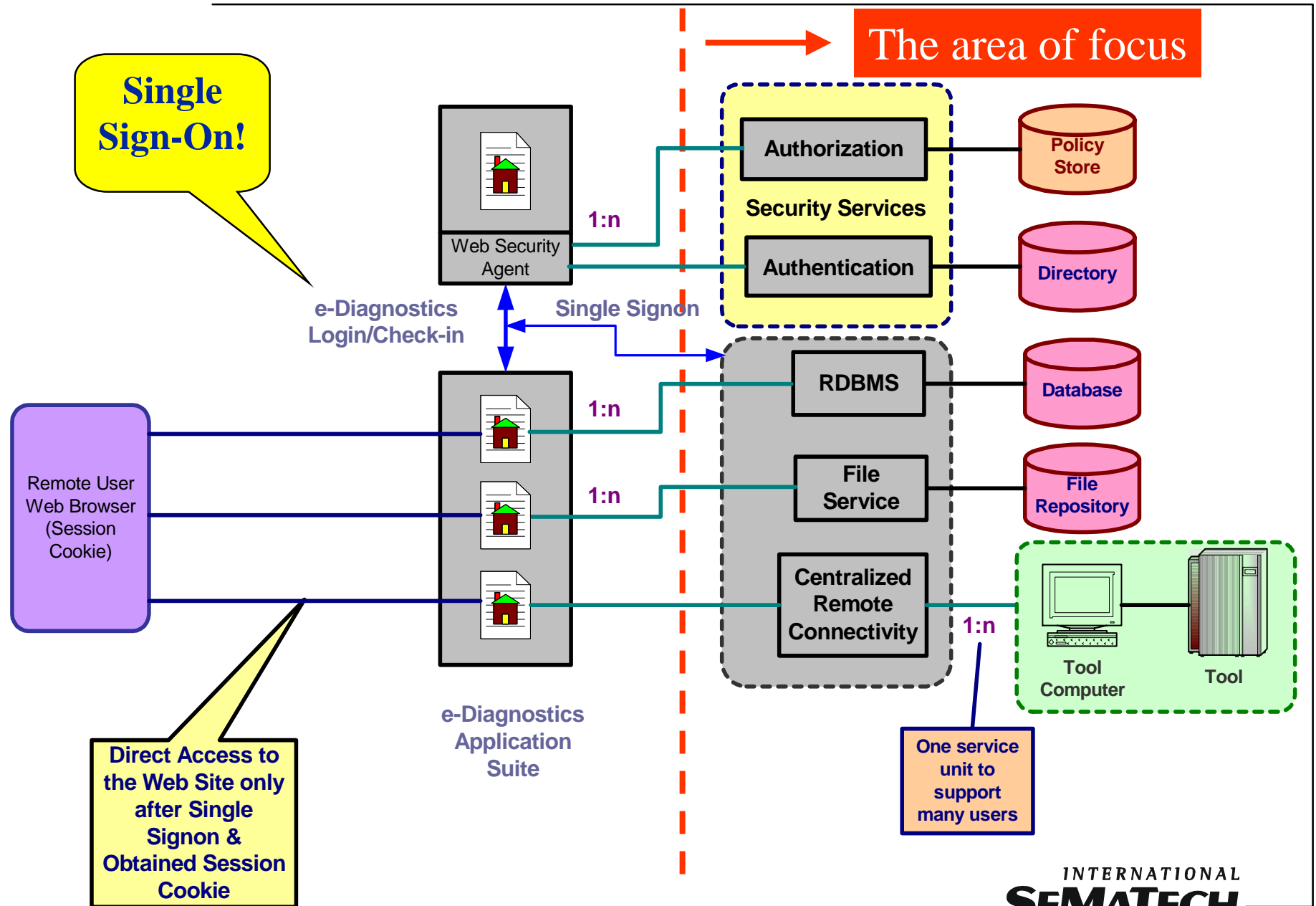
Red: Work in Progress with Plan to Complete by Q4' 2001

E-Diagnostics Hardware-Connectivity



Work in progress to harden the system!

Software-Logical Layer

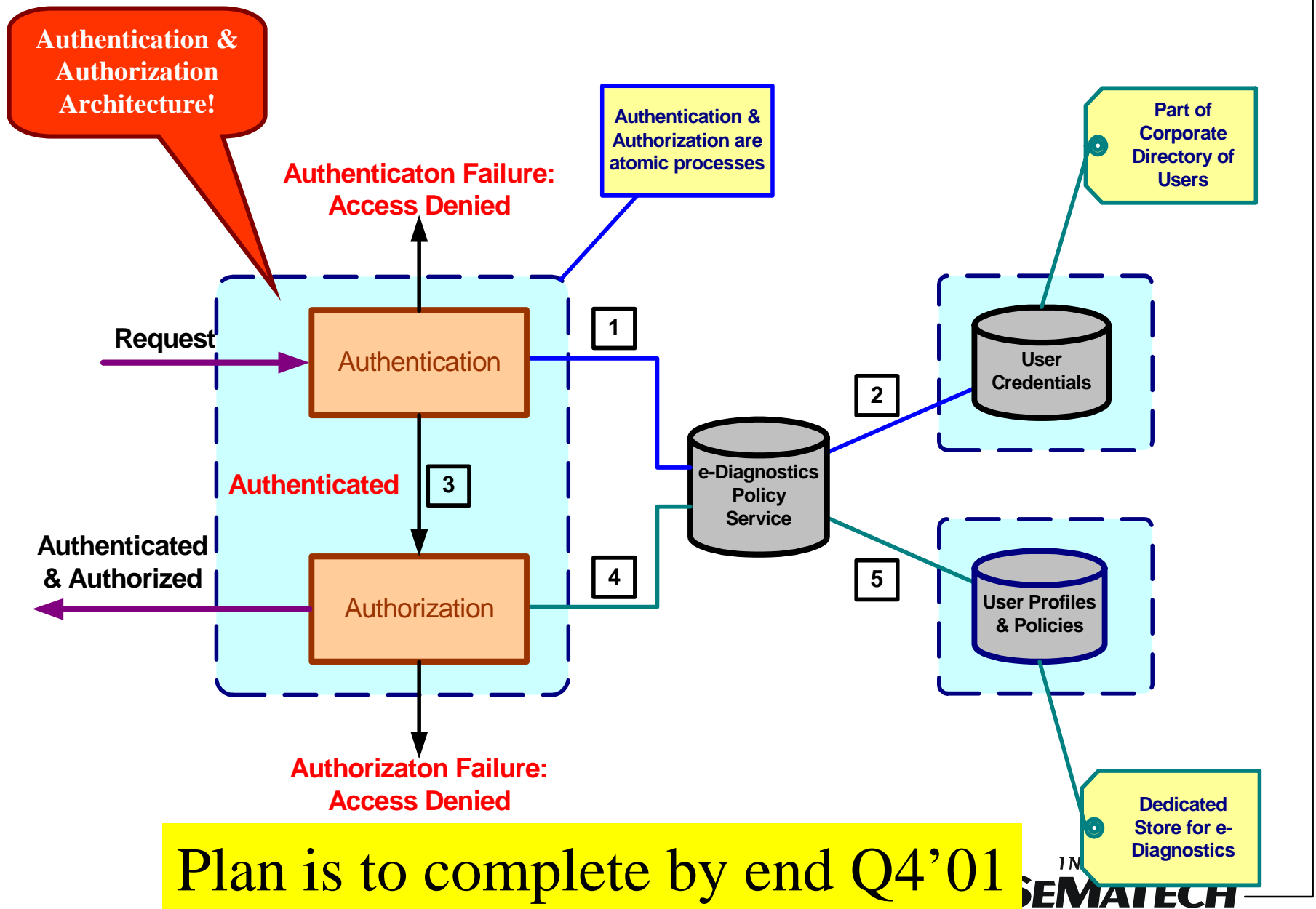


Software-Logical Layer

- **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 Signon:** 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...



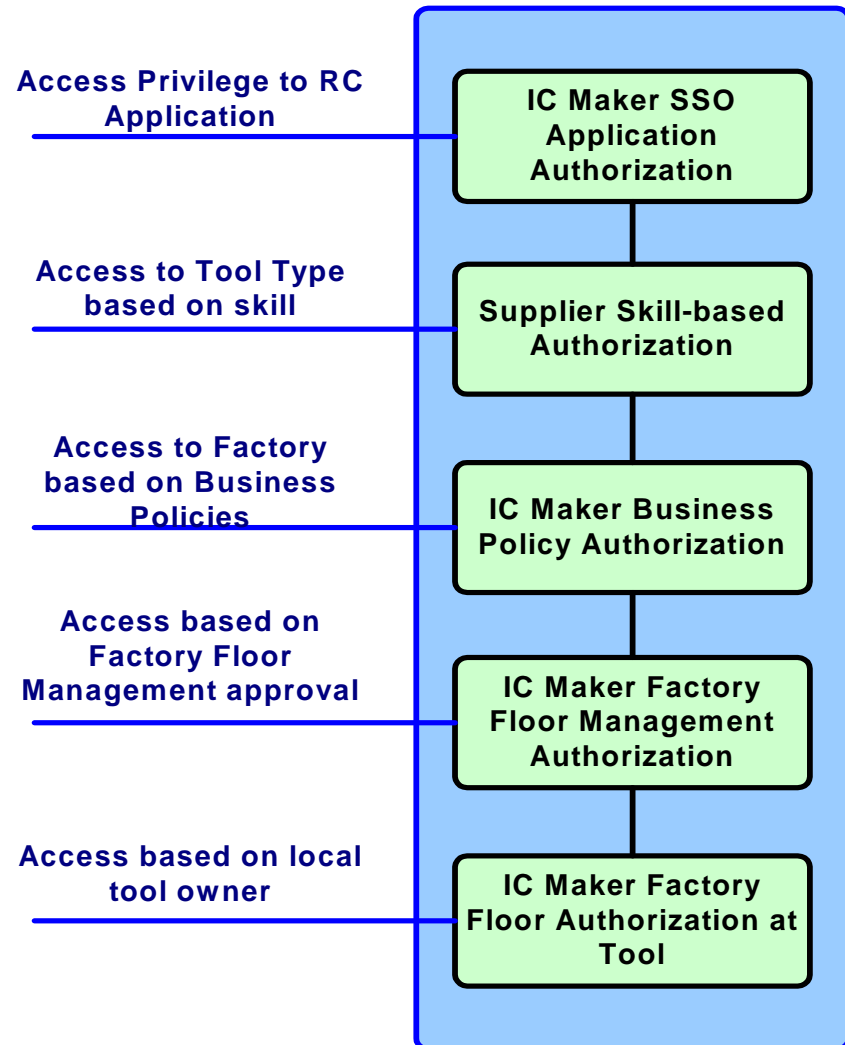
Plan is to complete by end Q4'01

Authorization Complexity

- **Authorization types:**
 - **Role based:** For user groups & privileges
 - **Rule based:** For business reasons such as time sensitivity, circumstances, etc.
- **Responsibilities:**
 - Various levels of IC Maker authorizations for task at hand
 - Supplier authorization also required to cover assignment of person of appropriate skill to task at hand.

Proper system design will resolve this complexity

Ex: Authorization for Remote Connectivity



System Hardening

- **Primarily targeting e-Diagnostics servers and equipment computers**
- **Commonly used industry wide practice – information available on the web.**
- **ISMT to create a standard template with focus on:**
 - Timely and well-tested software updates
 - Removal of unnecessary items such as login accounts, services
 - Tight configuration with appropriate file and directory permissions
 - Using effective audit and logging functions.

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 architecture**
 - 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