Security Reference Architecture

James (Jimmy) Darwin
James.Darwin@au.ibm.com

PulseANZ 2010

Meet the people who can help advance your infrastructure

Reference Architectures

- As part of the Time-to-Value Initiative, Reference Architectures have been identified as an emerging theme: Common customer deployment & usage patterns to facilitate earlier initial customer value.
  - Consistency moves us toward standard Reference Architectures with Management System deployments treated like SOA deployments
  - Repeatable, proven, robust patterns of deployment

- A reference architecture provides a proven template solution for an architecture for a particular domain. It also provides a common vocabulary with which to discuss implementations, often with the aim to stress commonality. [Wikipedia]

Reference Architecture

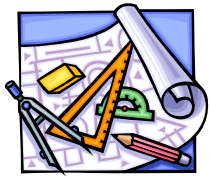
- Goals and Objectives
  - Provide a validated configuration through integration and scalability testing
  - Leverage *virtualization* as much as possible
  - Minimize the overall physical and virtual footprint without compromising performance
  - Reduce risks associated with one-of-a-kind configurations in both deployment and maintenance
  - Educate the field on these architectures and establish them as the de-facto standard recommended architecture
  - Recommend an ongoing governance cycle to maintain currency of these architectures.
  - Provide two platforms to choose from (AIX on P, and Linux on Intel)

Reference Architecture

- Reference Architectures Under Construction
  - Business Systems Management
  - Cloud Computing
  - Security
  - Service Process and Automation
  - IT Asset Management
  - Storage
  - Network Performance Management

IBM Security Framework & Blueprint

IBM Security Framework



IBM Security Blueprint

IBM Capabilities & Offerings

Business View	Technical View	Solution Architecture View
Security Domains	Foundational Security Mgmt Services	Platforms
	Common Security Infrastructure features	Components
		Configurations
Issues & Drivers	Standards & technologies	Principles & Practices

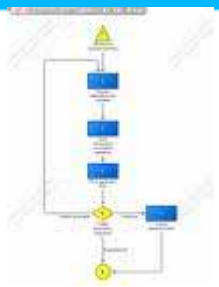
Describes the business landscape

Describes the technology landscape

Catalogs of integrated products, services and solutions

Client Briefings

External White Papers,



Best Practices / Guidance

RedBooks / RedGuides

Solution Architectures

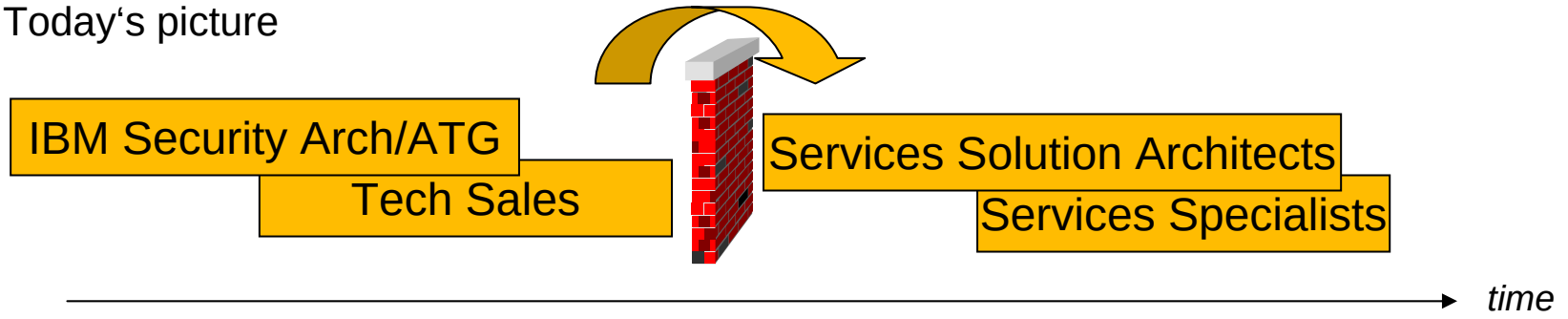
Product Documentation

Create a consistent technical approach, consistent terminology, and a consistent security “look and feel” across all security-related customer interactions

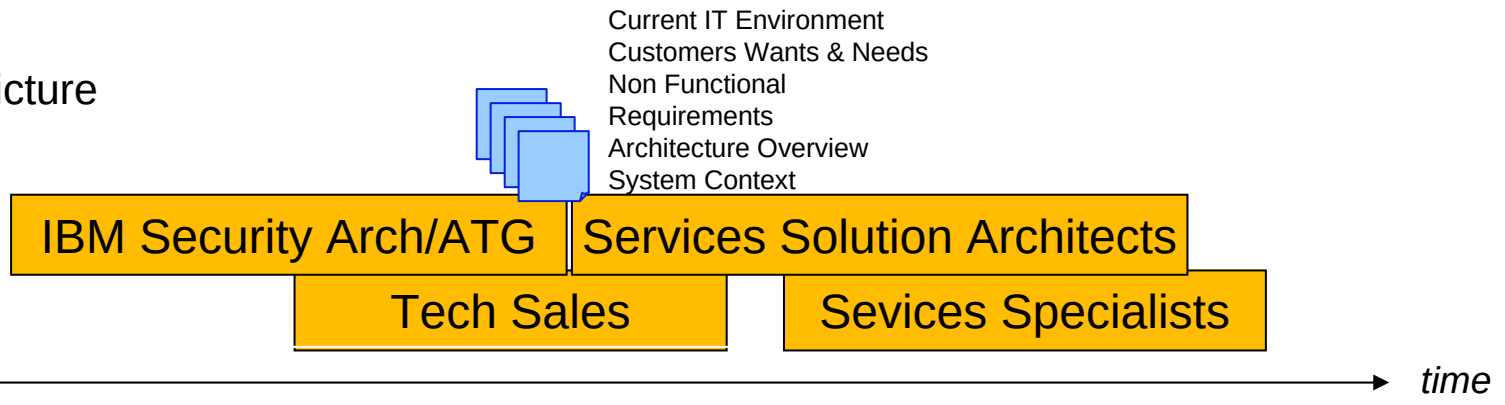
Addressing Customers Wants and Needs

We need to get better in Providing a smooth transition between organizations

Today‘s picture



Ideal picture



Contents of the Architecture Template based on GS Method Work Products

- Incorporated GS Method Work Products
  - ARC 301 ***Current IT Environment ****
  - BUS 314 Business/Process Drivers
  - BUS 320 Customers Wants & Needs
  - APP 130 ***Use Case Model ****
  - ARC 119 ***Non Functional Requirements ****
  - ARC 101 ***Architecture Overview ****
  - APP 011 ***System Context ****
  - ARC 100 ***Architectural Decisions ****
  - ARC 108 Component Model
  - ARC 113 Operational Model
  - ARC 111 ***Deployment Units ****

  - APP 306 ***Configuration Parameters ****
  - ARC 309 Principles - Policies and Guidelines
  - BUS 309 Process Definition
  - ARC 307 Enterprise Information Model
  - ARC 306 Data Stores
  - APP 110 Logical Data Model

Primary Work Products

Secondary Work Products

** Currently part of the draft Security Reference Architecture*

What do the Security Reference Architecture Work Products Provide

- a security *deployment* blueprint
- documents targeted at the trained security consultant level
- the format required for all significant Security Architecture and Solution Designs by Services Teams
- customer-specific environment descriptions, enterprise integration points, data component relationships, and known operational characteristics and configurations
- reviewed and approved by the IBM (DRB) and customers
- a “living document”
- recognition a “one-size-fits-all” approach is not feasible

Products & Components in Scope

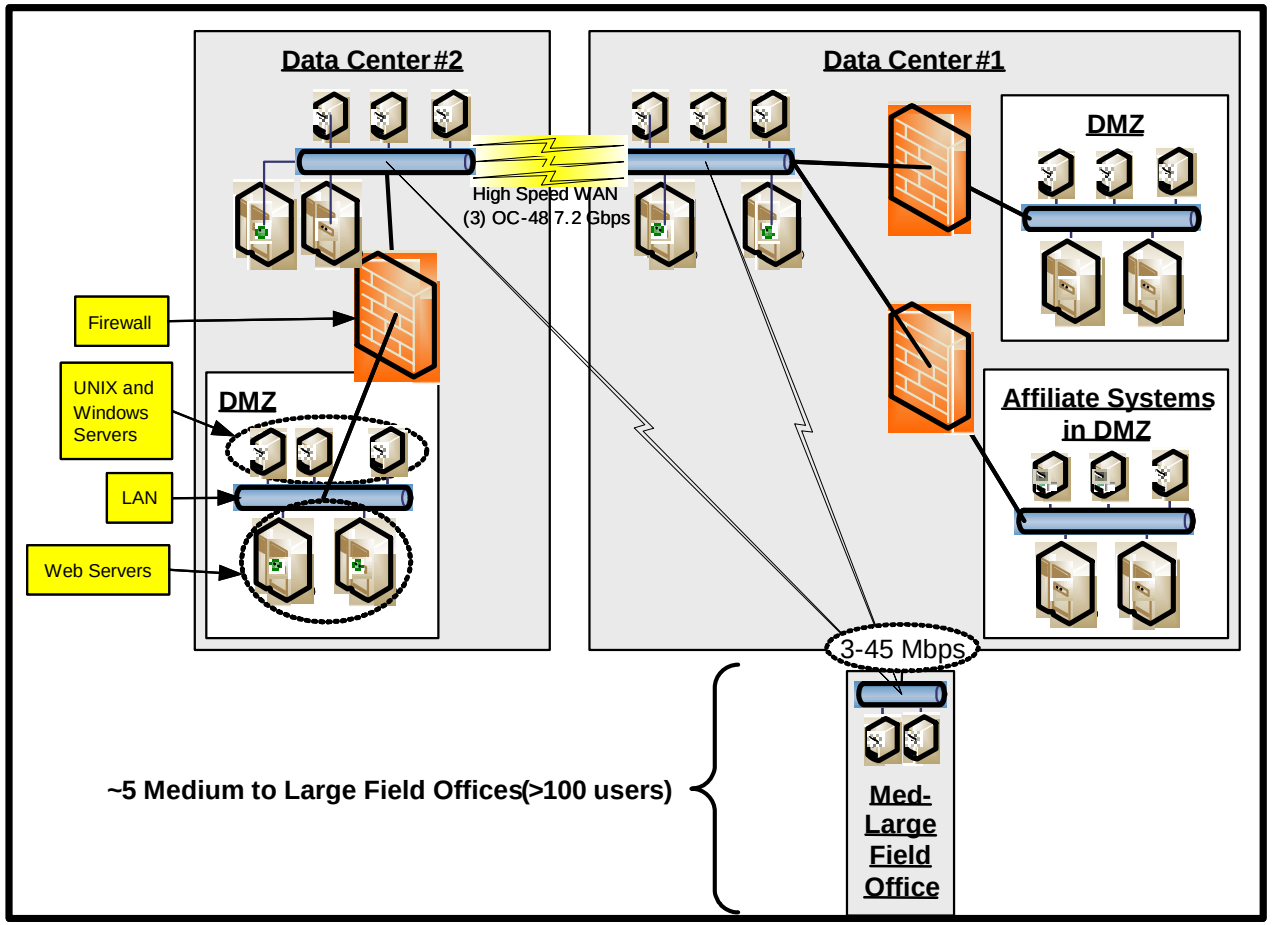
Products

- IBM Tivoli Access Manager for eBusiness 6.1.1 (TAMeb)
- IBM Tivoli Identity Manager 5.1 (TIM)
- IBM Tivoli Directory Server 6.2 (TDS)
- IBM Tivoli Directory Integrator 7.1 (TDI)
- IBM Tivoli Federated Identity Manager 6.2.1 (TFIM)
- IBM Tivoli Compliance Insight Manager 2.0 (TSIEM)

Next Additions

- IBM Tivoli Access Manager for Enterprise SSO 8.1 (TAMESSO)
- IBM Tivoli Key Lifecycle Manager v2.0 (TKLM)
- IBM Tivoli Security Policy Manager v7.x (TSPM)
- IBM Security Virutal Server Protection for VMware v1.0 (VSP)

Client IT Environment

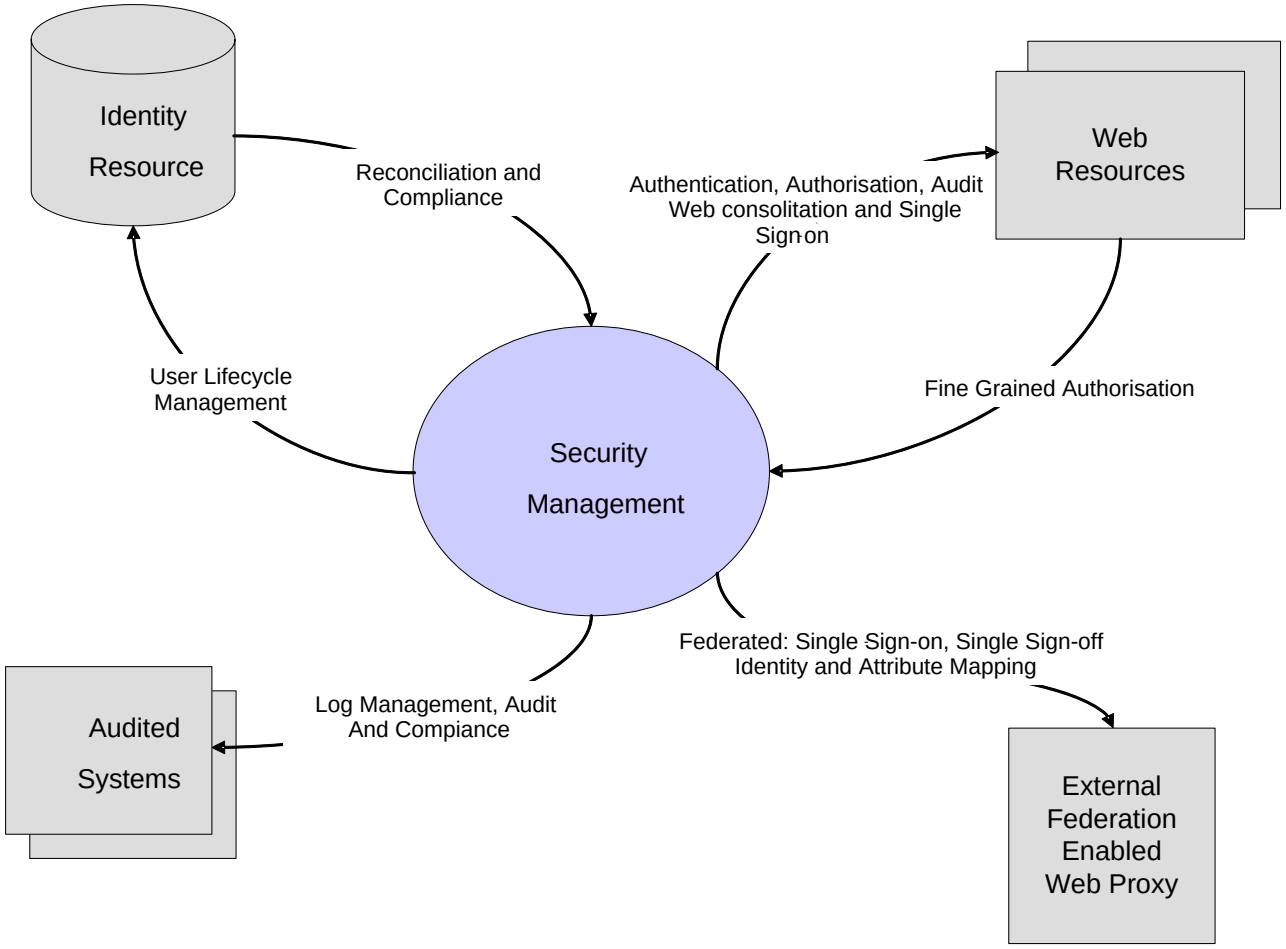


Total Servers	**3053**
AIX	167
Linux (RHEL)	121
Linux (SLES)	67
Solaris	288
Windows	2400
z/OS	10
Databases	**692**
Application	**1041**

Non Functional Requirements

Index	Requirement Name	Value(s)
NFR01	Maintainability	The system should allow for easy software upgrades with minimal outage. The outage should be restricted to no longer than one day, and allow for the use of a back up system for service continuity while the upgrade the taking place.
NFR02	High Availability	All components should be configured in a high availability configuration to eliminate single points of failure, and minimize solution outages.
NFR03	Disaster Recovery	The solution will be configured to be split across the two data centers where possible with failover from data center to data center in the event of a disaster, In addition, each data center needs to be able to run in a self sufficient manner should it become isolated from the other.
NFR04	Minimize Footprint	Stack multiple components within single operating system instances where possible to minimize both the number of physical and virtual servers required to run the Tivoli solution.
NFR05	Operating System(s)	All components should run on AIX (P-series) and Linux (X-series) where possible
NFR06	Virtualization	All components should be installed in virtual machines as opposed to standalone machines where possible
NFR07	Databases	All Databases should leverage the existing DB2 database farm whenever possible
NFR08	WebSphere Application Server	All WAS instances should leverage the existing WAS clusters where possible

System Context

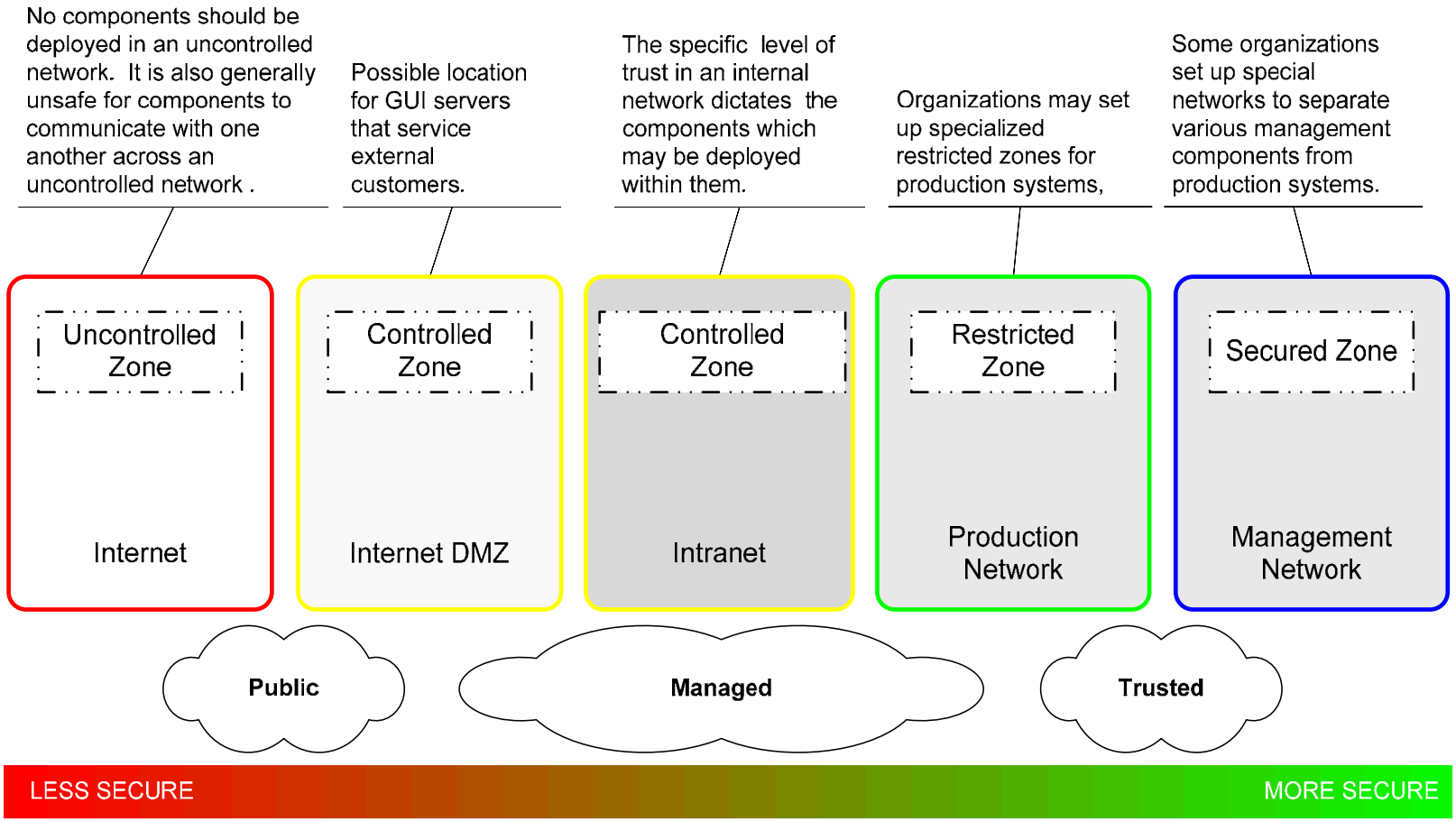


Architectural Decisions

- Where ever relevant choices exist, Architectural Decisions document the decision with a proper justification
- Examples:
  - High-availability is required for the authentication of users in the TAMeb environment
  - TIM will be used to manage the enterprise directory account data
  - The TAMeb infrastructure will support multiple locations for disaster recovery requirements
  - All web traffic will be go through the TAMeb WebSEAL Servers
  - Userid / Password authentication will be required for protected web resources
  - All access to sensitive data servers must be audited to a central log facility
  - All passwords must be encrypted in transit and at rest

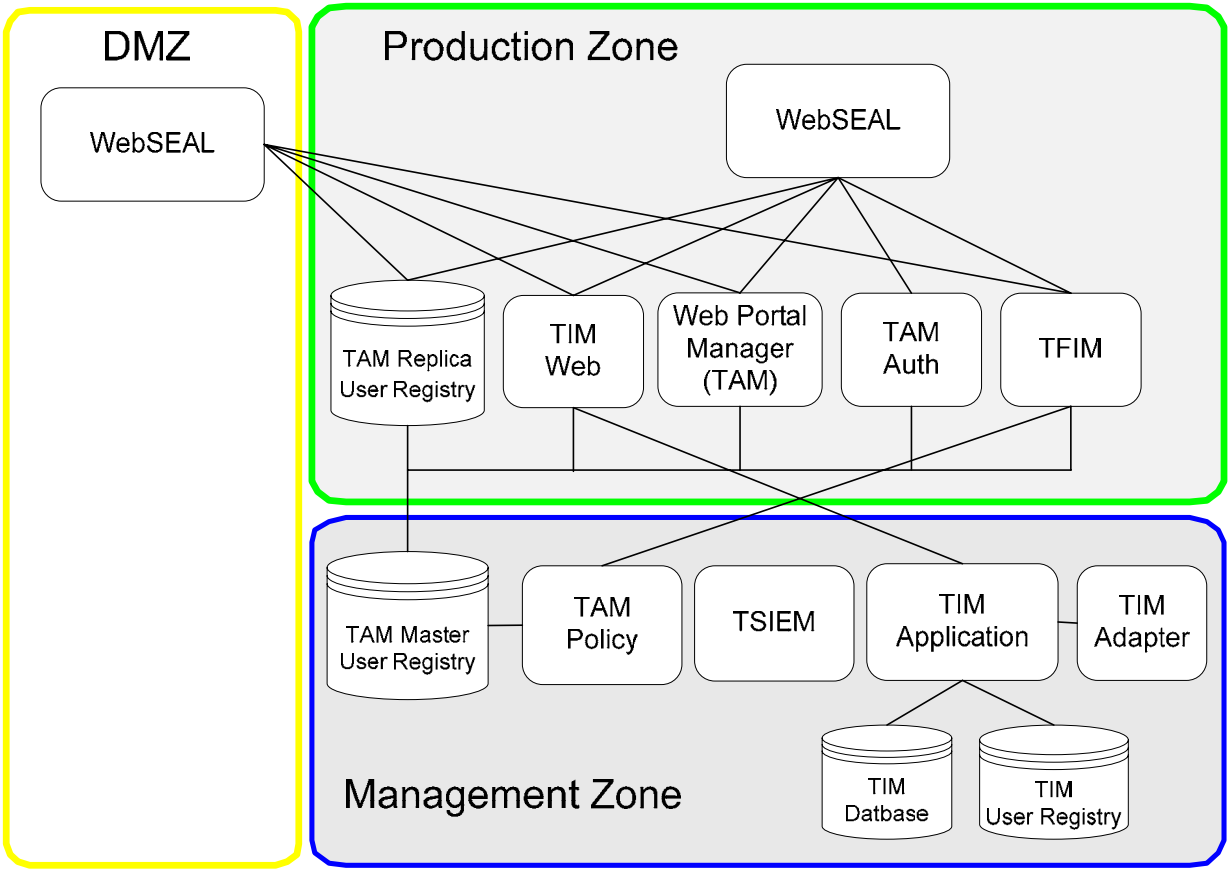
Subject Area	Area of Concern	**Topic**	Topic of Interest
Architectural Decision		**AD ID**	A unique identifier
Issue or Problem	A short description of the problem—what is being decided		
Assumptions	What is believed to be true about the context of the problem, constraints on the solution		
Motivation	Why this decision is important		
Alternatives	A list of alternatives and explanations		
Decision	The decision taken, possibly with references to related work products		
Justification	Why the decision was made and a list of compliance to Architecture Principles and explanations of deviations from compliance		
Implications	What impact the decision will have		
Derived requirements	A list of requirements that are generated by this decision		
Related Decisions	A list of related decisions		

Common Language



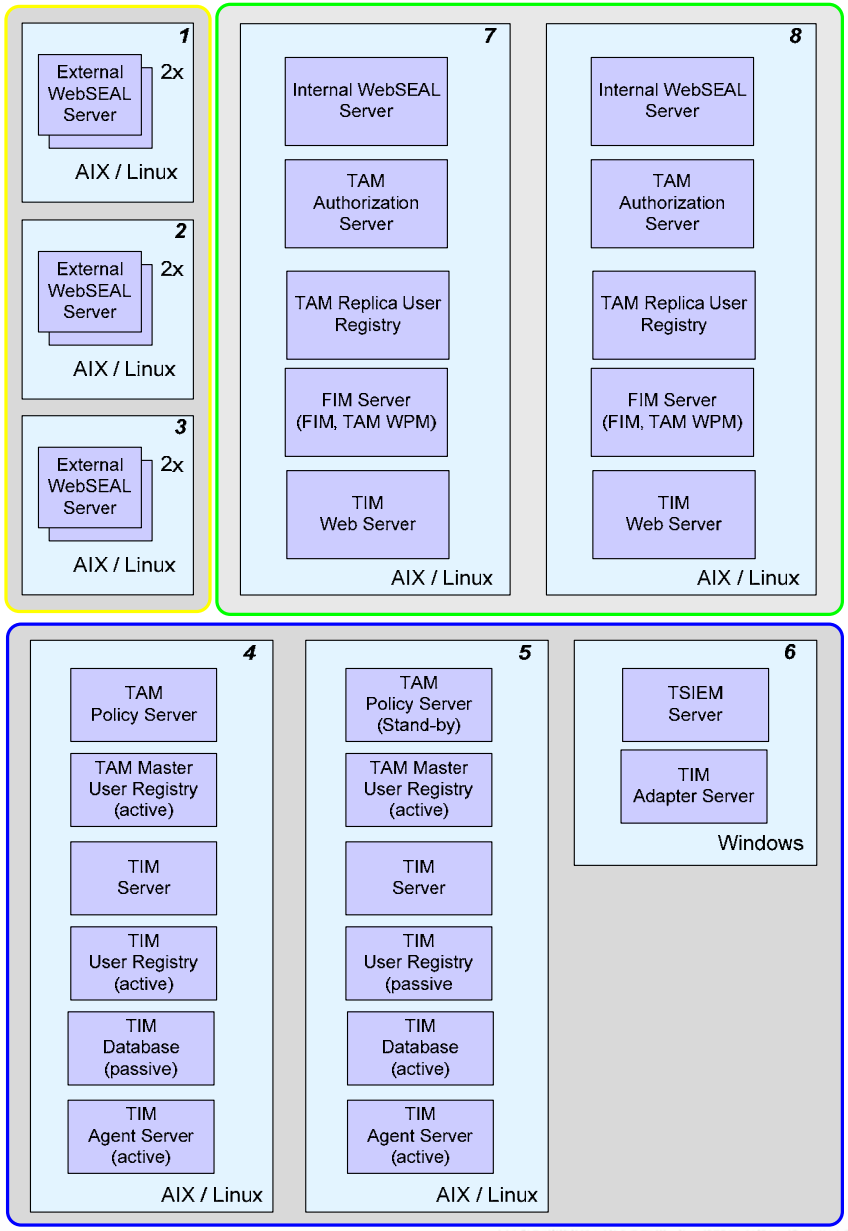
Architecture Overview

- Web Access Management
- Federated Single Sign-on
- Identity Management
- Security Information Management



Deployment Model

- DMZ Servers
- Managed Servers
- Production Servers



Configuration Parameter

- Configuration Parameters describes the selection and setting of values and options that customize a package or packages.
- Building on the rules and standards and the product characteristics, this chapter identifies, documents, and sets the parameters for a client-specific version of a product.

- Examples:
  - Installation paths used, permissions defined
  - Service accounts used
  - Naming Conventions
  - Product-specific configuration Parameters
  - TCP/IP Ports used
  - Performance Tuning Paramters
  - Password Policies

What Value Does the Reference Architecture Provided to Customers?

- Proven!
  - Based on customer implementatation patterns
  - Sized for the platform
  - Tested – by Development and the field
  - Reduce time-to-value
  - Reduce risk
  - Will lead to success

Questions / Comments?

Do you have feedback, or would you like to participate in this program?

Please contact:

James.Darwin@au.ibm.com

Trademarks and disclaimers

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries./ Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both. IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce. ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office. UNIX is a registered trademark of The Open Group in the United States and other countries. Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both. Other company, product, or service names may be trademarks or service marks of others. Information is provided "AS IS" without warranty of any kind.

The customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer.

Information concerning non-IBM products was obtained from a supplier of these products, published announcement material, or other publicly available sources and does not constitute an endorsement of such products by IBM. Sources for non-IBM list prices and performance numbers are taken from publicly available information, including vendor announcements and vendor worldwide homepages. IBM has not tested these products and cannot confirm the accuracy of performance, capability, or any other claims related to non-IBM products. Questions on the capability of non-IBM products should be addressed to the supplier of those products.

All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Some information addresses anticipated future capabilities. Such information is not intended as a definitive statement of a commitment to specific levels of performance, function or delivery schedules with respect to any future products. Such commitments are only made in IBM product announcements. The information is presented here to communicate IBM's current investment and development activities as a good faith effort to help with our customers' future planning.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.

Prices are suggested U.S. list prices and are subject to change without notice. Starting price may not include a hard drive, operating system or other features. Contact your IBM representative or Business Partner for the most current pricing in your geography.

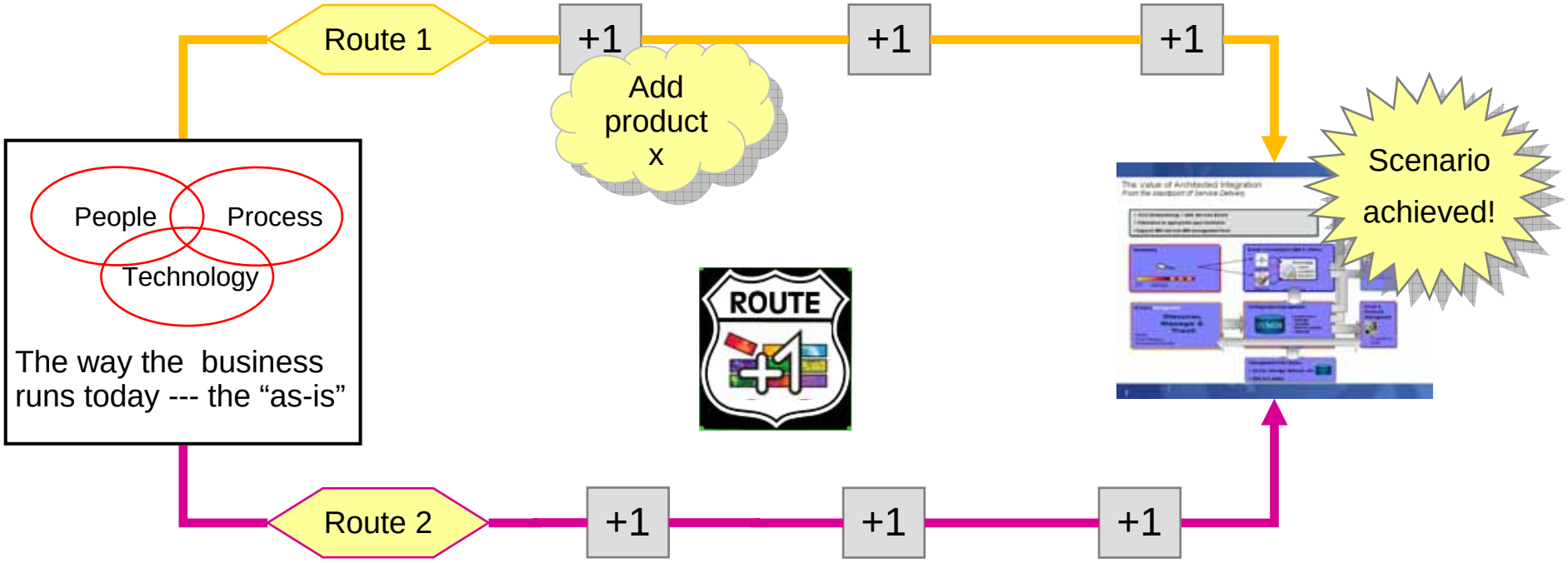
Photographs shown may be engineering prototypes. Changes may be incorporated in production models.

References in this document to IBM products or services do not imply that IBM intends to make them available in every country.

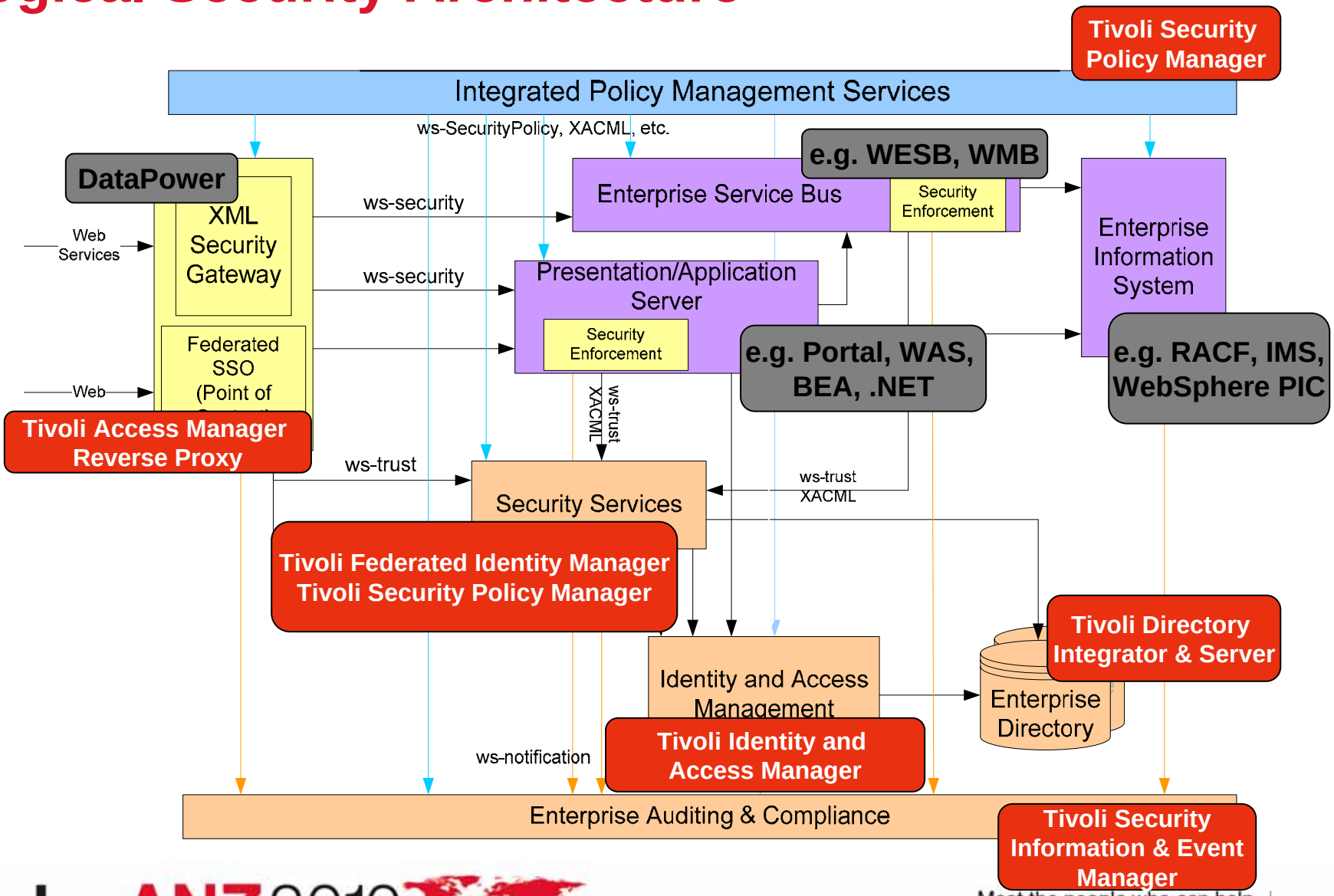
Trademarks of International Business Machines Corporation in the United States, other countries, or both can be found on the World Wide Web at http://www.ibm.com/legal/copytrade.shtml.

Reference Architectures and PlusOne

- A reference architecture is a desired end state configuration for a solution while the Plus One adoption routes provide a prescriptive methodology for deploying the solution, delivering incremental business value along the way.



Logical Security Architecture



IBM Security Framework

- The IBM Security Framework provides a broad view of security
  - Business problem oriented, focused on the “what”, not the “how”
  - Technology and service delivery / form-factor neutral
  - Translates into coarse-grained Business solutions, not into specific IT components or IT services
  - Solutions addressing problems from different domains tend to share common elements

IBM Security Blueprint Overview diagram

Architectural Principles

IBM Security Framework: Business Security Reference Model

- Governance, Risk, Compliance (GRC)
- People & Identity
- Data & Information
- Application & Process
- IT Infrastructure: Network, Server, End Point
- Physical Infrastructure

Foundational Security Management

- Software, System & Service Assurance
- Identity, Access & Entitlement Mgmt
- Data & Information Protection Mgmt
- Threat & Vulnerability Management
- IT Service Management
- Command and Control Mgmt
- Security Policy Management
- Risk & Compliance Assessment
- Physical Asset Management

Security Services and Infrastructure

- Security Info and Event Infrastructure
- Identity, Access & Entitlement Infrastructure
- Security Policy Infrastructure
- Cryptography, Key & Certificate Infrastructure
- Network Security
- Storage Security
- Host and End-point Security
- Application Security
- Service Management and Process Automation
- Physical Security
- IT Security Services and Mechanisms

- Security Service Level Objectives
- Code & Images / Designs
- Policies / Configuration Info and Registry
- Identities & Attributes / Resources
- Contexts / Data
- Security Events & Logs / Knowledge

IBM Security Blueprint – Architectural Principles Secure by Design

Architectural Principles

1. Openness
2. Security by default
3. Design for accountability
4. Design for regulations
5. Design for privacy
6. Design for extensibility
7. Design for sharing
8. Design for consumability
9. Multiple levels of protection
10. Separation of management, enforcement and accountability
11. Security is model-driven
12. Security-critical resources must be aware of their security context
13. Consistency in approaches, mechanisms and software components