

**Arizona Enterprise Architecture Target Technology Table**

Obsolete, Transitional*	Target* (Strategic)	Emerging*
<b>OSI Layer 1 – Physical</b>		
<b>Network</b>		
Coaxial cabling, Category 3 unshielded twisted pair (UTP), shielded twisted pair (STP), and 62.5/125-micron multimode fiber.	Category 5e UTP (supersedes Category 5 UTP), 50/125-micron multimode fiber, 8/125-micron single mode fiber.	Category 6 UTP, wireless.
Bus topology	Logical star topology	Logical meshed star topology
<b>Security</b>		
Open-door physical access	Keys, locks, badges, cameras, access logs, controlled access systems	IP-based access control systems, biometrics
<b>Platform</b>		
Platforms that employ proprietary protocols, gateways, as opposed to open-standard interfaces	SCSI, iSCSI	Trusted Platform
	Single application smart cards	Multi-function smart cards
<b>OSI Layer 2 – Data Link</b>		
<b>Network</b>		
Single-segment LANs, separate networks for different services (e.g., voice and data), separate dedicated networks for various user groups, proprietary protocols (e.g., SNA, Token Ring, Appletalk-addressing), FDDI, X.25, time-domain protocols (e.g., SDLC, HDLC)	Open-standards-based, multi-service networks; 100/1000 Ethernet; 802.11 LAN, 802.16 MAN Wireless Ethernet; Frame Relay; ATM	Packet- and cell-based wireless and satellite protocols, dynamic data-link level switching, and prioritization, 10G/40G Ethernet
Hub technology	Switched technology	
<b>Security</b>		
No Media Access Control Access Control Lists	Media Access Control Access Control Lists	
<b>OSI Layer 3 - Network</b>		
<b>Network</b>		
Proprietary protocols (e.g., IPX, AppleTalk-routing, DECnet)	IP; RIP; BGP; OSPF; IP switching; and DHCP.	IPv6
Separate networks for different services (e.g. voice and data), flat designs with unmanaged bridges, hubs,	Converged networks with prioritization for all services; switched, multi-segment design	Dynamic, network-level switching and prioritization
Fixed IP addressing		
<b>Security</b>		
Open, non-firewalled access Critical or Confidential data transmitted in clear formats	Integrated firewalls - Packet filtering, ICMP, Boundary Routers, static NAT, IPSec	
<b>OSI Layer 4 - Transport</b>		
<b>Network</b>		
Proprietary protocols (e.g., SPX, AppleTalk-Transport)	TCP, and UDP	
	Converged networks with prioritization for all services	Dynamic transport-level switching and prioritization
<b>Security</b>		
Open, non-firewalled access	Integrated firewalls - Stateful Inspection, dynamic NAT	
<b>OSI Layer 5 – Session</b>		

# Arizona Enterprise Architecture Target Technology Table

<b>Network</b>		
AppleTalk-session and DEC-dns	DNS	Dynamic, session-level switching and prioritization
<b>OSI Layers 6 – Presentation. 7 – Application</b>		
<b>Network</b>		
AppleTalk-filing, and DEC-lat	SNMP; RMON; SMTP	Dynamic, content-level switching and prioritization
<b>Security</b>		
Open, non-firewalled Web, FTP, and Mail Servers	Integrated firewalls - Application-proxy gateway, Proxy Servers, Dedicated Proxy Servers. FTP, S/MIME for mail servers, OpenPGP, Role-based administration, permissions, and rights. Smart cards, Kerberos	
Proprietary security products	Firewalled DNS, with services placed on DMZ, SSL	Multi-function smart cards Enterprise directory services - LDAP meta-directory with an OID tree
User selected passwords that do not conform to restrictive standards. Signs-on's that only work with a single platform or application User-based privileges	Standards-based platform sign-on with role-based administration  Industry standard and vendor neutral APIs for identification Strong password policy Token-based identification Public Key Certificates	Single sign-on across platforms, domains  Human Authentication API (HA-API)  Public Key Infrastructure Mobile agents
<b>Platform</b>		
	Platforms having open industry-standard operating systems, with imbedded security, and open-standard interfaces and drivers	Platforms having open industry-standard operating systems, with imbedded security, multifactor authentication, and open-standard interfaces and drivers
<b>OSI Layers 6 – Presentation. 7 – Application</b>		
<b>Platform</b>		
Platforms having proprietary operating systems without open-standard interfaces and drivers. For example: <ul style="list-style-type: none"> <li>o Mainframes without TCP/IP</li> <li>o Digital or analog PBXs /Key Systems requiring a separate network infrastructure</li> <li>o Voice mail systems without open APIs</li> <li>o Storage Area Networking with single-use, proprietary, fiber channel</li> <li>o Pagers, used concurrently with PDAs, radios, cell phones</li> <li>o Analog telephony devices</li> </ul>	Platforms having industry de facto standard operating systems, with imbedded security, and open-standard interfaces and drivers. For example: <ul style="list-style-type: none"> <li>o Mainframes with TCP/IP, SIP, Open APIs</li> <li>o Servers with TCP/IP, SIP, Open APIs</li> <li>o IP telephony with TCP/IP, SIP, Open APIs</li> <li>o Hybrid IP telephony (TDM/IP) systems with TCP/IP, SIP, Open APIs</li> <li>o Network Attached Storage</li> <li>o Direct Attached Storage</li> <li>o Storage Area Networking with multi-use access channels</li> <li>o Client devices (PCs, Network Computers, PDAs, etc.) with wired/wireless connectivity, TCP/IP and multi-function applications</li> </ul>	
Platform and Network Operating Systems that are unable to utilize a converged network infrastructure to access business applications	Platforms having niche proprietary operating systems, with imbedded security, and open-standard interfaces and drivers (requires exceptional business requirements)  SNMP management of platforms  Platforms deployed on target networks, with class	

## Arizona Enterprise Architecture Target Technology Table

of service (CoS) and quality of service (QoS)		
<b>Software</b>		
Traditional, monolithic State software applications deployed on proprietary server and client platforms (e.g., mainframe deployment requiring transitional version of OS with terminal access or terminal emulation access only, etc.)	n-tier distributed software applications emphasizing client (State employee, community of interest, public customer) productivity and performance enhancements and enablers (decision-making at the appropriate level) through self-service, self-administration, etc., utilizing browser-based client access deployed on Target Platform Architecture server, storage, and client devices (P100-S102)	Open, industry standard Web services, .NET, WSDL, XML, UDDI initiatives  Software applications hosted via ASPs
Client/server software applications deployed with "fat" client requirements	Traditional, monolithic State software applications with web-enabled, browser-based, client access.	
Business programming languages such as COBOL used in legacy software applications Manufacturer-specific programming languages Platform-specific programming languages such as assembler, etc Proprietary gateways, interfaces DCE H.320, H.323	Three-tier distributed software applications with access to n-tier architecture services  C++, Java™, Visual Basic®, etc.    Java™ and servlet software, COM™, DCOM™ CORBA, ORB (P100-S102), ISO/IEC 11179 SIP, SDP, SAP, RTSP	Object-oriented software IIOP
<b>OSI Layers 6 – Presentation. 7 – Application</b>		
<b>Software</b>		
Vendor/database-specific middleware with proprietary extensions	Open API (P100-S102)  Middleware: TPM, RPC, RMI, JMS, MOM  HTML, XHTML, XML (P100-S102)	J2EE™ EJB™ server-side deployment, COM+  EbXML secure exchange of information, UML™, SAML, XSL, CSS3, XSLT, DSML, SOAP, TLS
3270 terminal access to software	GUI presentation layer access to software as a precursor to browser-based access Browser-based access to software	Portal-based universal browser access to all services
Unmanaged software applications	Software applications that are manageable with SNMP-based management tools (P100-S101, P100-S102) LDAP directory services (P800-S820, P100-S102) Software application security (P800-S800 series)	Enterprise federated management tools Enterprise LDAP directory services
Flat file systems, ISAM, VSAM	RDBMS	OODBMS, ORDBMS
Vendor-specific SQL extensions	Open database connectivity: SQL, ODBC, OLE DB, NDMP, NFS, CIFS, JDBC (P100-S102) Database middleware that uses open database connectivity	
Vendor-specific database middleware with proprietary extensions Proprietary email systems, non-MIME-compliant email, proprietary, closed email directory services Proprietary, closed productivity software	Email services: SMTP, S/MIME, IMAP4, POP3  Productivity software with open APIs	Enterprise email directory services Productivity software conforming to IETF standards such as iCalendar, CAP, IPP, etc.

\* The terms "Obsolete, Transitional, Target (Strategic), and Emerging" as defined herein provide guidance regarding the status of specific architecture technologies.

➤ **Obsolete.** Arizona's EA strongly promotes that agencies employ a different technology. Agencies must not plan new

## Arizona Enterprise Architecture Target Technology Table

deployments of this technology and should develop a plan to replace this technology. This technology is typically outdated, no longer widely supported, and has been superseded by a newer, better technology.

- **Transitional.** Arizona's EA promotes other standard technologies. Agencies may presently be using this technology as a transitional strategy in movement to a target/strategic technology. This technology may be waning in use or no longer supported.
- **Target (Strategic).** Arizona's EA promotes use of this technology by agencies. New deployments of this technology are recommended.
- **Emerging.** Arizona's EA promotes only evaluative deployments of this technology. This technology may be in development or may require further evaluation.

*January 14, 2003*