9 Technical security architecture

9.1 Context

9.1.1 Time

Rate each item from 0 to 10, sum, and divide by 5 for an overall rating.

Item	*Rate*
Time zones associated with actions are tracked and logged.	
The time within context, or universal coordinated time (UTC) is used internally in system clocks, applications, and audit systems.	
Time relative to context is used when important to mission.	
Error types and magnitudes are tracked and where feasible accurate times are generated by atomic clocks, radio-based time synchronization, or network time protocol as appropriate.	
Differential time is used in synchronization and differential limits are tracked when critical to operations.	
Sum rates and divide by 5	

Startup	*Diligence*	*Typical*	*Excellent*	*Best*
2.5	5	5	7	10

9.1.2 Location

Rate each item from 0 to 10. Add ratings and divide by 14 for an overall rating.

Item	*Rate*
Network location determines large-scale controls.	
Zoning policies are used to create the large-scale topology of protection architecture.	
Addresses combined with related controls are used to differentiate systems and uses.	
Lines associated with telephone systems, terminal connectors, and direct or switched communications systems are used to indicate location and this location is then used to determine controls.	
Special phone numbers are used for special functions such as access to maintenance functions, and are restricted to connections from select remote telephone numbers.	

Item	*Rate*
Global Positioning System (GPS) locations are used to provide location information that can be correlated with other information to provide functions ranging from routing to assistance calls.	
GPS is used to limit access and to provide location-based authentication.	
Location is correlated with time for travel rates and to associate physical and logical access.	
Physical locations are associated with devices and protective barriers and are used as a basis for allowing or denying access.	
Known physical locations have known protective conditions that allow extraordinary access based on facilities protection, personnel characteristics, and so forth.	
Local access to consoles is used to grant maintenance access.	
Logical location codifies a set of conditions associated with a device or operating environment that is used to associate a level of trust.	
Proxy servers or similar mechanisms provide a local presence that is used to gain access associated with a location that may differ from the actual location of the individual performing the process.	
Location changes are used to detect exception conditions based on physical impossibility.	
Location information is retained in audit records.	
Add rates and divide by 15 to get the rating	

Startup	*Diligence*	*Typical*	*Excellent*	*Best*
2	3	3	5	7

9.1.3 Purpose

Rate each item from 0 to 10. Add ratings and divide by 11 for an overall rating.

Item	*Rate*
Authority is used as a basis for authorization through an ownership process.	
Context is used as a basis for use.	
Applicability of an action to a purpose is the basis for allowing use.	
Risk associated with access is used as a reason for denying use.	
Utility is balanced with risk as a basis for use.	

Item	*Rate*
Access is refused by default for medium and high risk systems.	
A rationale that makes sense to the owner of the content is used as the basis for use.	
Human judgments over classes of uses and applications authorized for those uses is used by owners.	
Rationale for use is a logical argument balancing risks against benefits.	
Explanation is used to provide additional details to the decision-maker.	
Validity of explanations, rational, and basis are subject to external inspection and audit.	
Add ratings and divide by 11 for an overall rating.	

Startup	*Diligence*	*Typical*	*Excellent*	*Best*
3	5	6	8	10

9.1.4 Identity

	Issue	*Rate*
Name	Names are uniquely associated with all of the identified items of interest, whether they be individuals or things.	
Type	Types are associated with identity information. There are people, things, and subtypes associated with them.	
Properties	Properties include linkage to roles and rules, locations, times, capabilities to authenticate, biometric properties, and other properties associated those identities.	
Basis	Basis for identity is used as a surety metric.	
Surety	The extent to which an identity has been authenticated is used as a basis to determine authorization.	
Rating	Total (sum ratings / 5)	

Startup	*Diligence*	*Typical*	*Excellent*	*Best*
1	7	7	9	10

9.1.5 Behavior

Item	*Rate*
Actions are tracked in behavioral modeling and analysis systems and are used to make protection decisions.	
Sequences of actions are used to detect deviations and known behavioral patterns.	
Combinations of system, world situation and event sequences lead to the action that should take place.	
Inputs to systems are examined to seek to understand situation and behavioral interactions.	
Outputs from systems are verified for acceptability.	
State information is used to understand behavior in context.	
Changes to states and behaviors are examined together to identify behavioral anomalies.	
Total ratings / 7	

Startup	*Diligence*	*Typical*	*Excellent*	*Best*
0	1	3	7	10

9.1.6 Method

Item	*Rate*
Hardware is preferred to software for higher surety systems.	
Software is preferred for flexibility and cost in low surety systems.	
Route controls are designed to use the path from place to place to increase the level of certainty that content is what it is considered to be.	
Means are considered in determining assurance levels.	
Transforms seal information and are used to prove to those that can verify the seal or unseal the information that the creator had the transform.	
Protocols are used to differentiate request types.	
Packet or Line are used to differentiate how content arrives or is sent and these are controlled to limit paths.	
Physicality is used in certain interfaces, such as the console interfaces, to differentiate actions that are allowed.	

Item	*Rate*
Voice, Data, and Video paths are differentiated so that certain functions can only be performed over certain types of interfaces or with certain types of content.	
Total rates and divide by 8	

Startup	*Diligence*	*Typical*	*Excellent*	*Best*
2	4	5	7	10

9.1.7 Roll-up

Enter ratings from each area in the ratings column. Determine the level achieved based on ratings by selecting the highest answer less than or equal to the rating.

Area	*Rating*	*Level*	*S*	*D*	*T*	*E*	*B*
Time			2.5	5	5	7	10
Location			2	3	3	5	7
Purpose			3	5	6	8	10
Identity			1	7	7	9	10
Behavior			0	1	3	7	10
Method			2	4	5	7	10
Total / 6			1.75	4.1	4.8	7.1	9.5

Failure to meet due diligence in any area means that overall rating is not diligent.