



## TECHNOLOGY AREA

DEFINITION	
<i>Name</i>	Identification and Authentication
<i>Description</i>	<p>Identification and Authentication is a technical measure that prevents unauthorized people (or unauthorized processes) from accessing an IT system.</p> <p>Identification is a unique way of identifying each individual user or process (e.g., a unique user name or ID).</p> <p>Authentication is the mechanism that verifies that an individual is who they claim to be. Verification is based on one or more of the following:</p> <ul style="list-style-type: none"> <li>• Something known (e.g., a password or pin);</li> <li>• Something carried (e.g., a smart card or a token);</li> <li>• Something the individual is (e.g., biometrics – like a fingerprint).</li> </ul>
<i>Rationale</i>	<p>State agencies have the responsibility of protecting confidential data and information systems. Identification and Authentication are the first lines of defense to protect enterprise system assets from unauthorized access, destruction or theft.</p> <p>Hardware platforms, operating systems, application-specific constraints, and overall financial or confidentiality risk are factors that influence the need for identification and authentication controls.</p> <p>System and application developers are responsible for designing strong authentication into the systems they build, and individual users are responsible for assisting in the protection of the systems they use.</p>
<i>Benefits</i>	<ul style="list-style-type: none"> <li>• Identification and authentication helps prevent unauthorized persons from entering enterprise IT systems. If identification and authentication are not handled correctly, they are the weakest link in the protection of enterprise systems and data.</li> <li>• Identification and authentication provides user accountability and auditable trails of user access.</li> </ul>
ASSOCIATED ARCHITECTURE LEVELS	
<i>Specify the Domain Name</i>	Security
<i>Specify the Discipline Name</i>	Technical Controls
KEYWORDS	
<i>List Keywords</i>	Passwords, password controls, digital signatures, access controls, access cards, smart cards, tokens, biometrics, user name, user ID, PIN, logon ID, 2FA

ASSOCIATED COMPLIANCE COMPONENTS			
<i>List the Compliance Component Names</i>	<ul style="list-style-type: none"> <li>• Password Controls</li> <li>• Access Controls</li> </ul>		
ASSOCIATED PRODUCT COMPONENTS			
<i>List the Product Component Names</i>			
CURRENT STATUS			
<i>Provide the Current Status</i>	<input type="checkbox"/> <i>In Development</i>	<input type="checkbox"/> <i>Under Review</i>	<input checked="" type="checkbox"/> <i>Approved</i> <input type="checkbox"/> <i>Rejected</i>
AUDIT TRAIL			
<i>Creation Date</i>	02/13/2003	<i>Date Approved / Rejected</i>	4/18/2019
<i>Reason for Rejection</i>			
<i>Last Date Reviewed</i>	2/27/2019	<i>Last Date Updated</i>	
<i>Reason for Update</i>			