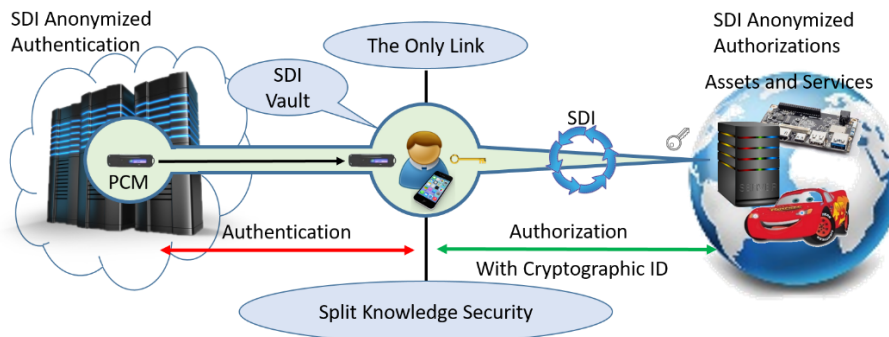
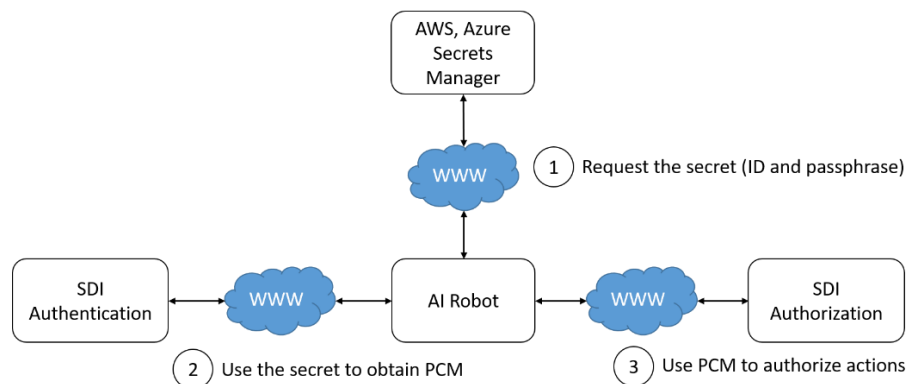


# AI Identity

AI (Artificial Intelligence) agents/robots are getting increasingly popular in business, the military, and personal activities. For years, software was considered tooling for users and would assume the user's permissions to access resources. In the same way, automation robots would always be activated by humans, so they would be given instructions on what to do and what to access, and for that purpose, the operator's identity would be used. AI agents/robots don't need that supervision because, to the extent of their training, they can act autonomously, so they should have their own identity to which policies and permissions would apply.



The SDI (Secure Digital Identity) platform provides identity verification using a cryptographic link (proxy) to the true identity. Humans can prove themselves with what they know (password and other confidential personal information), what they have (device, token), and what they are (biometric measurements). AI agents/robots cannot provide any of those three that would be unique to them. Even robotic devices powered by AI would have the same problem as devices used by humans: a lack of uniqueness. When working with SDI, humans can prove their identity to the SDI authentication service and thus obtain their unique PCM (Personal Cryptographic Matter) to be used to extend the reach of their identity to the SDI authorization services with certainty and privacy.



The AI agents/robots, on the other hand, can prove the possession of a secret (ID and a passphrase) stored on a Secrets Manager service, such as AWS or Azure, and use that secret to authenticate with the SDI authentication service to obtain their relevant PCM. From that point on, the AI agent/robot can accomplish what humans can: obtain resources from the cloud, gain access to physical objects, or have their own user permissions on a computer.