Identity & Credential Life-cycle

Industrial Technology Working Group

Michael J. Mossbarger

ENT Foundation Inc.

mike@ent.net

The following use case is designed to explore the life-cycle of an identity in an industrial network. Such identities may include network actors such as 1) machines, 2) users, 3) groups, 4) software process triggers, or 5) data files. Each identity has a basic life-cycle that includes 1) issuance, 2) renewal, and 3) deactivation. Issuance could be defined as the process that creates a unique identity/identifier and key; verifies the identity of the actor; and attaches the identity/identifier and key to the actor. Renewal could be defined as the invalidation of lost or compromised private keys with all affected actors in the system; the re-issuance of new keys; attaching the new keys to the subject actors; and the distribution of new private keys to all affected actors in the system. Deactivation could be defined as the invalidation of out of service identities/identifiers and keys with all affected actors in the system.

Technology/Utilities/UC002A: Issuance to a new sensor array	
Vignette	A new sensor array is being integrated into the platform where it will be used. The array must have a unique, secure identity to be installed in the platform to enable resolution, authentication, communication, security, etc.
Actors	Sensor Array with Gateway/Scalable Edge Node Sensor Data Engineer Maybe a Security Officer
Event	The new sensor array is delivered to the utility where it will be installed to monitor the operating metrics of a motor generator.
Pre-/Post-Conditions	Pre: Array is functional. Post: Array is securely connected. Nominal operation.
Technology	Communication mechanism available between array and network.
Fit Criteria	Array is authentically identified by the network. Network is authentically identified to Array. Reliability of new key(s) integrity. Operation nominal.
Scenario	1. Array is calibrated, etc. and ready for installation. 2. Engineer installs API, etc. which will allow the new array to connect to the larger network.

	3. Engineer creates/links identity for the array into the system. 4. Engineer creates/requests credentials for array. 5. Engineer configures array's access control to recognize appropriate administrator and peer entities. 6. Array synchronizes with system. 7. Array-sourced data is authenticated by appropriate peered entity.

Technology/Utilities/UC002B: Compromised asymmetric machine private key and renewal	
Vignette	Upon discovery that embedded array private keys have been compromised due to malware, compromised certificates are invalidated in the system and new certificates are established.
Actors	Sensor Array System administrator Malware
Event	Malware is identified as being present in a sensor array. This array collects, aggregates and transmits critical data. The malware is using the affected device's private keys to sign invalid data transmissions. Immediate replacement of compromised certificates is vital.
Pre-/Post-Conditions	Pre: Sensors and data node use embedded certificates with public/private key pairs for credentialing. Malware has been identified as residing on this sensor array only. Malware has access to private key on array. Key is compromised. Post: Compromised keys and corresponding certificates have been invalidated with all actors in the system. Malware has been removed. New certificates have been established for all compromised devices. The sensor array has a new secure private key.
Technology	Communication mechanism available between system administrator and all devices in sensor array. Asymmetric key cryptography.
Fit Criteria	Reliability of new keys' integrity
Scenario	1. Malware is discovered on array. 2. System administrator invalidates compromised array certificate(s). 3. Administrator resets array into known state, clearing malware. 4. Administrator updates array logic to prevent re-infection. 5. Array notifies administrator of new private key. 6. Administrator authorizes new certificate(s) for array. 7. New certificates are distributed to all actors in the system. 8. System returns to nominal operation.

Technology/Utilities/UC002C: Compromised anchor key	
Vignette	A physical break in has occurred and evidence is found that the storage location of a high level key has been accessed. Key is compromised.
Actors	System administrator

	Emergency IT remediation force Thousands of affected machines
Event	Chief system administrator's office was physically entered while he was out for the evening. His computer stores an anchor key which allows administrators access to move updates to critical sensor arrays in the multiple locations. There is evidence that his computer has been accessed which means this anchor key is compromised. If the compromised sensor arrays' private keys aren't immediately invalidated there could be wide spread vulnerability to these critical systems.
Pre-/Post-Conditions	Pre: Sensors and data node use embedded certificates with public/private key pairs for credentialing.. Storage location for sensor anchor key has been accessed. Attacker had/has access to anchor key. Key is compromised. Post: All compromised keys and corresponding certificates have been invalidated with all actors in the system. New certificates have been established for all compromised devices. Affected sensors are operational.
Technology	Communication mechanism available between system administrator and all devices in various sensor arrays. Asymmetric key cryptography.
Fit Criteria	Reliability of new keys' integrity
Scenario	1. Break in and compromise of anchor key is discovered. 2. System administrator brings all IT staff in around the clock to address this emergency need. 3. Team invalidates compromised array certificates. 4. Affected arrays resent into known state to ensure that any potential compromise has been remedied. 5. Administrative team updates arrays logic to prevent re-infection. 6. Arrays notify various administrators of new private keys. 7. Administrators authorize new certificates for arrays. 8. New certificates are distributed to all actors in the system. 9. System returns to nominal operation.

Technology/Utilities/UC002D: Deactivation of array	
Vignette	Array's useful life has been reached. It is being replaced and will no longer be operational in the system.
Actors	Sensor Array System administrator
Event	Array is being readied for removal.
Pre-/Post-Conditions	Pre: Nominal operation. Array is active. Post: Array's credentials have been deactivated with all affected actors. Array has been removed.
Technology	Communication mechanism available between system administrator and all

	devices in sensor array.
Fit Criteria	99% reliability that key is deactivated
Scenario	1. System admin invalidates device certificates. 2. Network recognizes invalidated array credentials. 3. Array is removed.