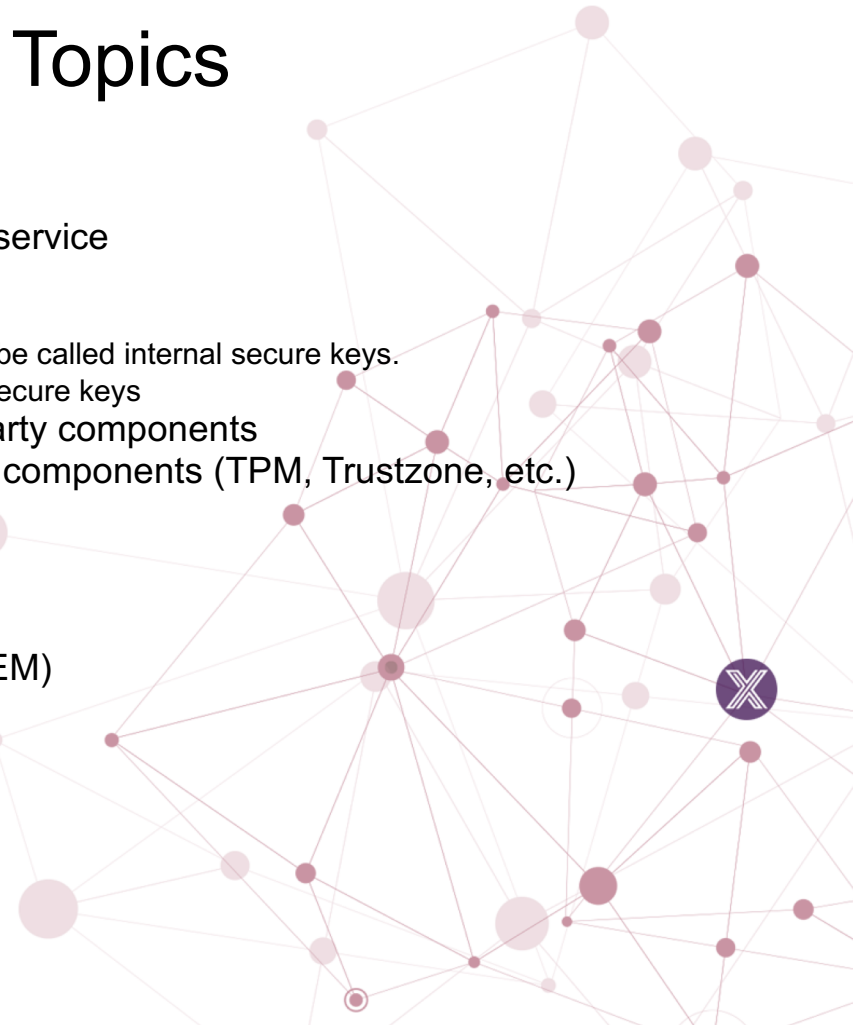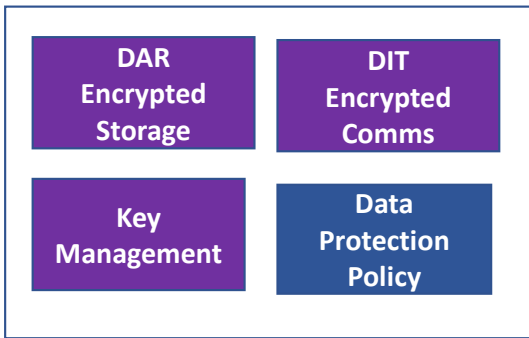# Delhi Discussion Topics

- What's Next for Delhi Discussion Points
  - Enhance Boot Strap Method for master RoT key for security service
  - Key Management Service additional features
    - Add create key
    - Add key management for keys that will not leave service. These will be called internal secure keys.
    - Add supported crypto services that will be supported using internal secure keys
  - Chain of Trust – Define Abstraction layer for pluggable 3rd party components
  - Attestation – Define Abstraction layer for pluggable 3rd party components (TPM, Trustzone, etc.)
  - Audit - Security event logging
  - Define Device Security Plan - Onboarding, connectivity
  - Define Integration Plan with Systems Management
  - Security Monitoring - Provide foundation for 3rd party visibility & monitoring (e.g. SIEM)
  - Integrated public CA support - Provide abstraction for access to 3rd party CAs
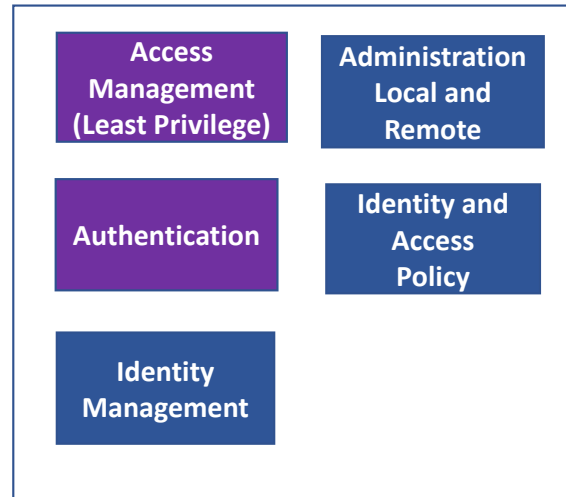 - Security Architecture
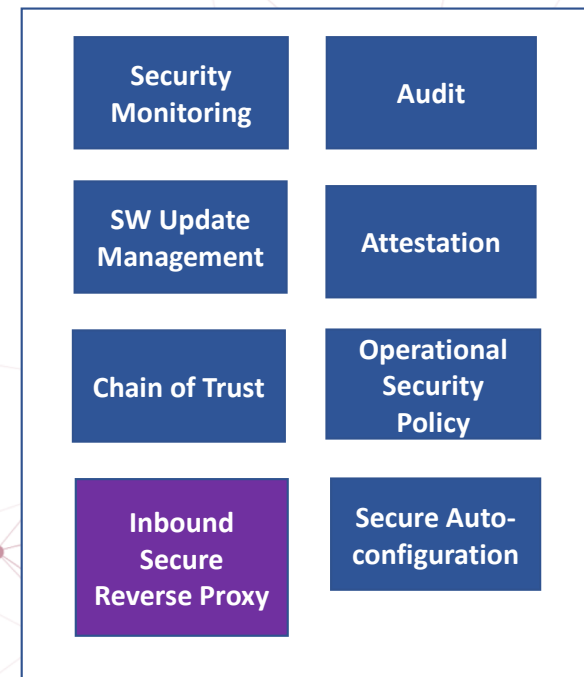
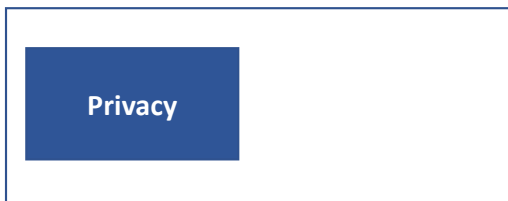# EdgeX Security High Level Architecture Services

Data Protection

DAR Encrypted Storage	DIT Encrypted Comms
Key Management	Data Protection Policy

Identity and Access

Access Management (Least Privilege)	Administration Local and Remote
Authentication	Identity and Access Policy
Identity Management	

Operational Security

Security Monitoring	Audit
SW Update Management	Attestation
Chain of Trust	Operational Security Policy
Inbound Secure Reverse Proxy	Secure Auto-configuration

Guidelines

Privacy

Element in purple are partially included in California release

edgexfoundry.org | @edgexfoundry