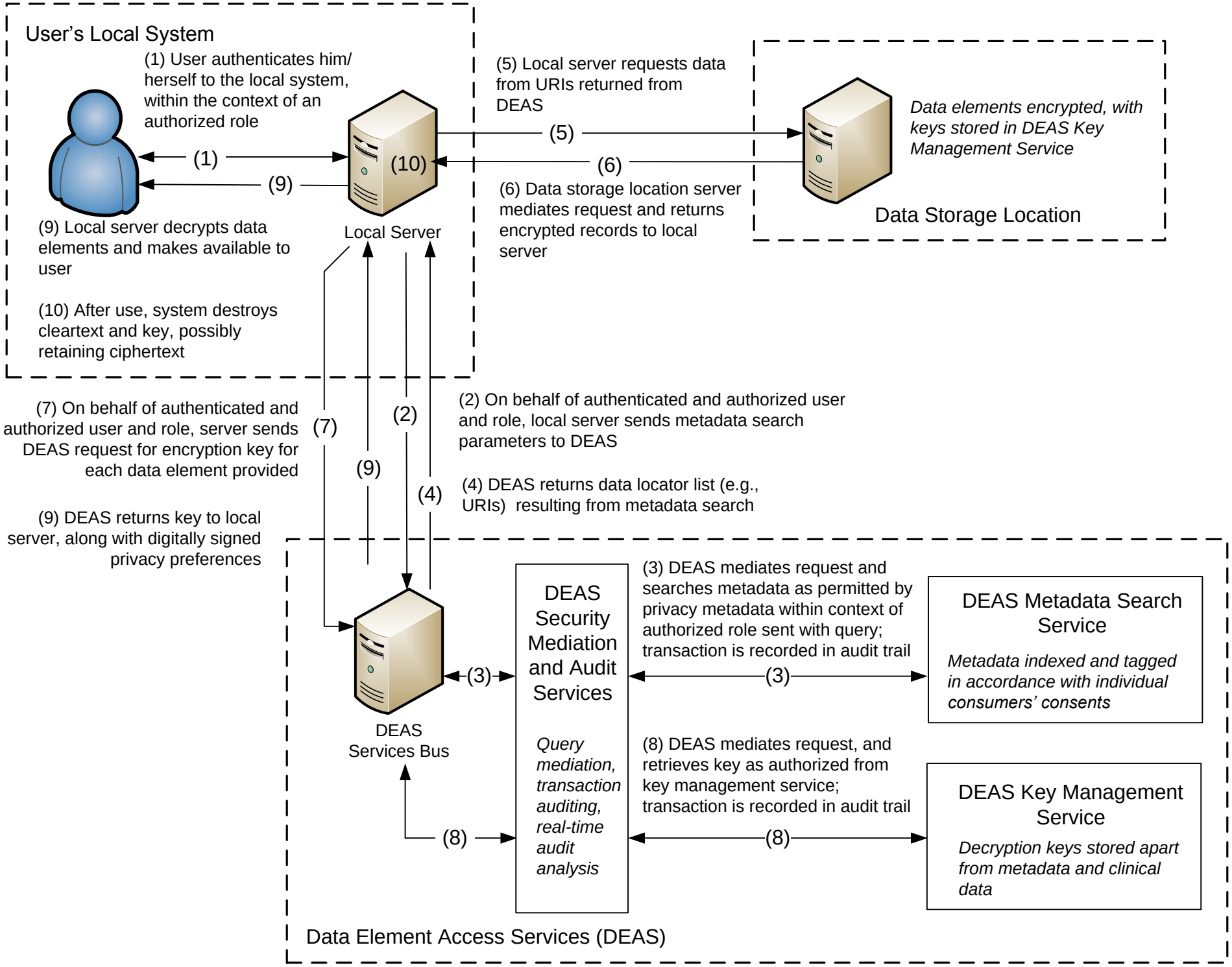
User's Local System
(1) User authenticates him/ herself to the local system, within the context of an authorized role
(1)
(9)
(10)
Local Server
(9) Local server decrypts data elements and makes available to user
(10) After use, system destroys cleartext and key, possibly retaining ciphertext
(5) Local server requests data from URIs returned from DEAS
(5)
(6)
(6) Data storage location server mediates request and returns encrypted records to local server
Data elements encrypted, with keys stored in DEAS Key Management Service
Data Storage Location
(7) On behalf of authenticated and authorized user and role, server sends DEAS request for encryption key for each data element provided
(7)
(2)
(9)
(4)
(2) On behalf of authenticated and authorized user and role, local server sends metadata search parameters to DEAS
(4) DEAS returns data locator list (e.g., URIs) resulting from metadata search
(9) DEAS returns key to local server, along with digitally signed privacy preferences
DEAS Services Bus
(3)
DEAS Security Mediation and Audit Services
Query mediation, transaction auditing, real-time audit analysis
(3) DEAS mediates request and searches metadata as permitted by privacy metadata within context of authorized role sent with query; transaction is recorded in audit trail
(3)
DEAS Metadata Search Service
Metadata indexed and tagged in accordance with individual consumers' consents
(8)
(8) DEAS mediates request, and retrieves key as authorized from key management service; transaction is recorded in audit trail
(8)
DEAS Key Management Service
Decryption keys stored apart from metadata and clinical data
Data Element Access Services (DEAS)