This protocol is between metadata server (MDS), client (C), and key distribution server (KDS) for a file with root key K_R and user A. We assume that KDS is given private key KR_A, which is paired with public key KU_A.

MDS	:	a meta data server.
C	:	a client or a computation node.
KDS	:	a key distribution server.
A	:	a user or an application.
KR_A	:	the private key for A.
KU_A	:	the public key for A.
(bs, d, i, j)	:	block size bs, depth d, range i, j.

Key request:

$$\begin{array}{rcl}
C \rightarrow MDS & : & \text{open request} \\
MDS \rightarrow C & : & E_{KU_A}(K_R) \\
C \rightarrow KDS & : & \{E_{KU_A}(K_R), \mathsf{range}(bs, d, i, j), \text{identification of } C\} \\
KDS \rightarrow C & : & K_{i,j} \\
C \rightarrow MDS & : & E_{KU_C}(K_{i,j}) \quad \text{(as a cache for } C\text{.)}
\end{array}$$

- identification of C might be $E_{KR_C}(bs, d, i, j)$ (signed range).
- the entire message in $C \rightarrow KDS$ might be encrypted by KU_{KDS}.
- MDS can be implemented as extended attributes.
- C does not have KR_A.
- KDS has KR_A.