(1) Origin generates *n* shared keys *k* (origin already has a public key PK and private key PK^{-1})

(2) Origin generates $HMAC_{k1}(URL)$, $\{content\}_{k1}$, $\{cert\}_{k1}$, …, $HMAC_{kn}(URL)$, $\{content\}_{kn}$, $\{cert\}_{kn}$

(3) Cache nodes pull $HMAC_{k1}(URL)$, $\{content\}_{k1}$, $\{cert\}_{k1}$, …, $HMAC_{kn}(URL)$, $\{content\}_{kn}$, $\{cert\}_{kn}$