

ABSTRACT

PARAMETER BASED KEY DERIVATION

Systems and methods for authentication generate keys from secret credentials shared between authenticating parties and authenticators. Generation of the keys may involve utilizing specialized information that, as a result of being used to generate the keys, renders the generated keys usable for a smaller scope of uses than the secret credential. Further, the key generation may involve multiple invocations of a function where each of at least a subset of the invocations of the function results in a key that has a smaller scope of permissible use than a key produced from a previous invocation of the function. Generated keys may be used as signing keys to sign messages. One or more actions may be taken depending on whether a message and/or the manner in which the message was submitted complies with restrictions of the key's use.

Figure 1