During the full authentication session, Fast_ID(0) and MK(0) are used for the first round of iterative AVs generating operation.

New AVs Database

AVs Database

New AVs Database

AP

Local Authentication Agent (LAA)

AVs Database

RADIUS/AAA Server

Authentication Vectors Distributor (AVD)

Counter_A(i) Nonce_A(i) Fast_ID(i-1) MK(i-1)

SHA-1

MK(i)

PRF

K_auth(i) K_encr(i)

Counter_A(i) Nonce_A(i) Fast_ID(i) MK(i)

Sha-1

MK(i)

PRF

K_auth(i) K_encr(i)

Counter_A(i) Nonce_A(i) Fast_ID(i) MK(i)

SHA-1

MK(i)

PRF

K_auth(i) K_encr(i)

Counter_A(i) Nonce_A(i) Fast_ID(i) MK(i)

SHA-1

MK(i)

PRF

K_auth(i) K_encr(i)

Counter_A(i) Nonce_A(i) Fast_ID(i) MK(i)

SHA-1

MK(i)

PRF

K_auth(i) K_encr(i)

Counter_A(i) Nonce_A(i) Fast_ID(i) MK(i)

SHA-1

MK(i)

PRF

K_auth(i) K_encr(i)

Counter_A(i) Nonce_A(i) Fast_ID(i) MK(i)

SHA-1

MK(i)

PRF

K_auth(i) K_encr(i)

Counter_A(i) Nonce_A(i) Fast_ID(i) MK(i)

SHA-1

MK(i)

PRF

K_auth(i) K_encr(i)

Counter_A(i) Nonce_A(i) Fast_ID(i) MK(i)

SHA-1

MK(i)

PRF

K_auth(i) K_encr(i)

Counter_A(i) Nonce_A(i) Fast_ID(i) MK(i)

SHA-1

MK(i)

PRF

K_auth(i) K_encr(i)

Counter_A(i) Nonce_A(i) Fast_ID(i) MK(i)

SHA-1

MK(i)

PRF

K_auth(i) K_encr(i)

Counter_A(i) Nonce_A(i) Fast_ID(i) MK(i)

SHA-1

MK(i)

PRF

K_auth(i) K_encr(i)

Counter_A(i) Nonce_A(i) Fast_ID(i) MK(i)

SHA-1

MK(i)

PRF

K_auth(i) K_encr(i)

Counter_A(i) Nonce_A(i) Fast_ID(i) MK(i)

SHA-1

MK(i)

PRF

K_auth(i) K_encr(i)

Counter_A(i) Nonce_A(i) Fast_ID(i) MK(i)

SHA-1

MK(i)

PRF

K_auth(i) K_encr(i)

Counter_A(i) Nonce_A(i) Fast_ID(i) MK(i)

SHA-1

MK(i)

PRF

K_auth(i) K_encr(i)

Counter_A(i) Nonce_A(i) Fast_ID(i) MK(i)

SHA-1

MK(i)

PRF

K_auth(i) K_encr(i)

Counter_A(i) Nonce_A(i) Fast_ID(i) MK(i)

SHA-1

MK(i)

PRF

K_auth(i) K_encr(i)

Counter_A(i) Nonce_A(i) Fast_ID(i) MK(i)

SHA-1

MK(i)

PRF

K_auth(i) K_encr(i)

Counter_A(i) Nonce_A(i) Fast_ID(i) MK(i)

SHA-1

MK(i)

PRF

K_auth(i) K_encr(i)

Counter_A(i) Nonce_A(i) Fast_ID(i) MK(i)

SHA-1

MK(i)

PRF

K_auth(i) K_encr(i)

Counter_A(i) Nonce_A(i) Fast_ID(i) MK(i)

SHA-1

MK(i)

PRF

K_auth(i) K_encr(i)

Counter_A(i) Nonce_A(i) Fast_ID(i) MK(i)

SHA-1

MK(i)

PRF

K_auth(i) K_encr(i)

Counter_A(i) Nonce_A(i) Fast_ID(i) MK(i)

SHA-1

MK(i)

PRF

K_auth(i) K_encr(i)

Counter_A(i) Nonce_A(i) Fast_ID(i) MK(i)

SHA-1

MK(i)

PRF

K_auth(i) K_encr(i)

Counter_A(i) Nonce_A(i) Fast_ID(i) MK(i)

SHA-1

MK(i)

PRF

K_auth(i) K_encr(i)

Counter_A(i) Nonce_A(i) Fast_ID(i) MK(i)

SHA-1

MK(i)

PRF

K_auth(i) K_encr(i)

Counter_A(i) Nonce_A(i) Fast_ID(i) MK(i)

SHA-1

MK(i)

PRF

K_auth(i) K_encr(i)

Counter_A(i) Nonce_A(i) Fast_ID(i) MK(i)

SHA-1

MK(i)

PRF

K_auth(i) K_encr(i)

Counter_A(i) Nonce_A(i) Fast_ID(i) MK(i)

SHA-1

MK(i)

PRF

K_auth(i) K_encr(i)

Counter_A(i) Nonce_A(i) Fast_ID(i) MK(i)

SHA-1

MK(i)

PRF

K_auth(i) K_encr(i)

Counter_A(i) Nonce_A(i) Fast_ID(i) MK(i)

SHA-1

MK(i)

PRF

K_auth(i) K_encr(i)

Counter_A(i) Nonce_A(i) Fast_ID(i) MK(i)

SHA-1

MK(i)

PRF

K_auth(i) K_encr(i)

Counter_A(i) Nonce_A(i) Fast_ID(i) MK(i)

SHA-1

MK(i)

PRF

K_auth(i) K_encr(i)

Counter_A(i) Nonce_A(i) Fast_ID(i) MK(i)

SHA-1

MK(i)

PRF

K_auth(i) K_encr(i)

Counter_A(i) Nonce_A(i) Fast_ID(i) MK(i)

SHA-1

MK(i)

PRF

K_auth(i) K_encr(i)

Counter_A(i) Nonce_A(i) Fast_ID(i) MK(i)

SHA-1

MK(i)

PRF

K_auth(i) K_encr(i)

Counter_A(i) Nonce_A(i) Fast_ID(i) MK(i)

SHA-1

MK(i)

PRF

K_auth(i) K_encr(i)

Counter_A(i) Nonce_A(i) Fast_ID(i) MK(i)

SHA-1

MK(i)

PRF

K_auth(i) K_encr(i)

Counter_A(i) Nonce_A(i) Fast_ID(i) MK(i)

SHA-1

MK(i)

PRF

K_auth(i) K_encr(i)

Counter_A(i) Nonce_A(i) Fast_ID(i) MK(i)

SHA-1

MK(i)

PRF

K_auth(i) K_encr(i)

Counter_A(i) Nonce_A(i) Fast_ID(i) MK(i)

SHA-1

MK(i)

PRF

K_auth(i) K_encr(i)

Counter_A(i) Nonce_A(i) Fast_ID(i) MK(i)

SHA-1

MK(i)

PRF

K_auth(i) K_encr(i)

Counter_A(i) Nonce_A(i) Fast_ID(i) MK(i)

SHA-1

MK(i)

PRF

K_auth(i) K_encr(i)

Counter_A(i) Nonce_A(i) Fast_ID(i) MK(i)

SHA-1

MK(i)

PRF

K_auth(i) K_encr(i)

Counter_A(i) Nonce_A(i) Fast_ID(i) MK(i)

SHA-1

MK(i)

PRF

K_auth(i) K_encr(i)

Counter_A(i) Nonce_A(i) Fast_ID(i) MK(i)

SHA-1

MK(i)

PRF

K_auth(i) K_encr(i)

Counter_A(i) Nonce_A(i) Fast_ID(i) MK(i)

SHA-1

MK(i)

PRF

K_auth(i) K_encr(i)

Counter_A(i) Nonce_A(i) Fast_ID(i) MK(i)

SHA-1

MK(i)

PRF

K_auth(i) K_encr(i)

Counter_A(i) Nonce_A(i) Fast_ID(i) MK(i)

SHA-1

MK(i)

PRF

K_auth(i) K_encr(i)

Counter_A(i) Nonce_A(i) Fast_ID(i) MK(i)

SHA-1

MK(i)

PRF

K_auth(i) K_encr(i)

Counter_A(i) Nonce_A(i) Fast_ID(i) MK(i)

SHA-1

MK(i)

PRF

K_auth(i) K_encr(i)

Counter_A(i) Nonce_A(i) Fast_ID(i) MK(i)

SHA-1

MK(i)

PRF

K_auth(i) K_encr(i)

Counter_A(i) Nonce_A(i) Fast_ID(i) MK(i)

SHA-1

MK(i)

PRF

K_auth(i) K_encr(i)

Counter_A(i) Nonce_A(i) Fast_ID(i) MK(i)

SHA-1

MK(i)

PRF

K_auth(i) K_encr(i)

Counter_A(i) Nonce_A(i) Fast_ID(i) MK(i)

SHA-1

MK(i)

PRF

K_auth(i) K_encr(i)

Counter_A(i) Nonce_A(i) Fast_ID(i) MK(i)

SHA-1

MK(i)

PRF

K_auth(i) K_encr(i)

Counter_A(i) Nonce_A(i) Fast_ID(i) MK(i)

SHA-1

MK(i)

PRF

K_auth(i) K_encr(i)

Counter_A(i) Nonce_A(i) Fast_ID(i) MK(i)

SHA-1

MK(i)

PRF

K_auth(i) K_encr(i)

Counter_A(i) Nonce_A(i) Fast_ID(i) MK(i)