It is an GSS-API/SASL mechanism to do username/password/OTP authentication.

Based on SCRAM – only minor modifications to protocol for sending the OTP to server

Use-case 1: sites with username/password authentication (CRAM-MD5 or SCRAM) used for IMAP+SMTP that wants to add an OTP factor easily

“easily” means (at least) without having to change existing credentials (username/password)
;; from RFC 5802
client-final-message-without-proof =
   channel-binding "," nonce [""," extensions]

;; variant used by CROTP
otp = "o=" saslname
client-final-message-without-proof =
   channel-binding "," nonce "," otp [""," extensions]

Examples:
o=755224 (OATH HOTP)
o=dteffujedcflcindvdbrblehecuitvjkjevvehjd (YubiKey)
Open questions

• How important is confidentiality of the OTP? Validation protocols and deployments rarely confidentiality protect OTPs and it “works”. TLS? GSS_Wrap?

• Could an EAP mechanism be used together with GSS-EAP instead? EAP-GTC “kind of” supports OTP but it works poorly in practice.

• Generally, is there support for working on two-factor authentication in GSS-API/SASL?