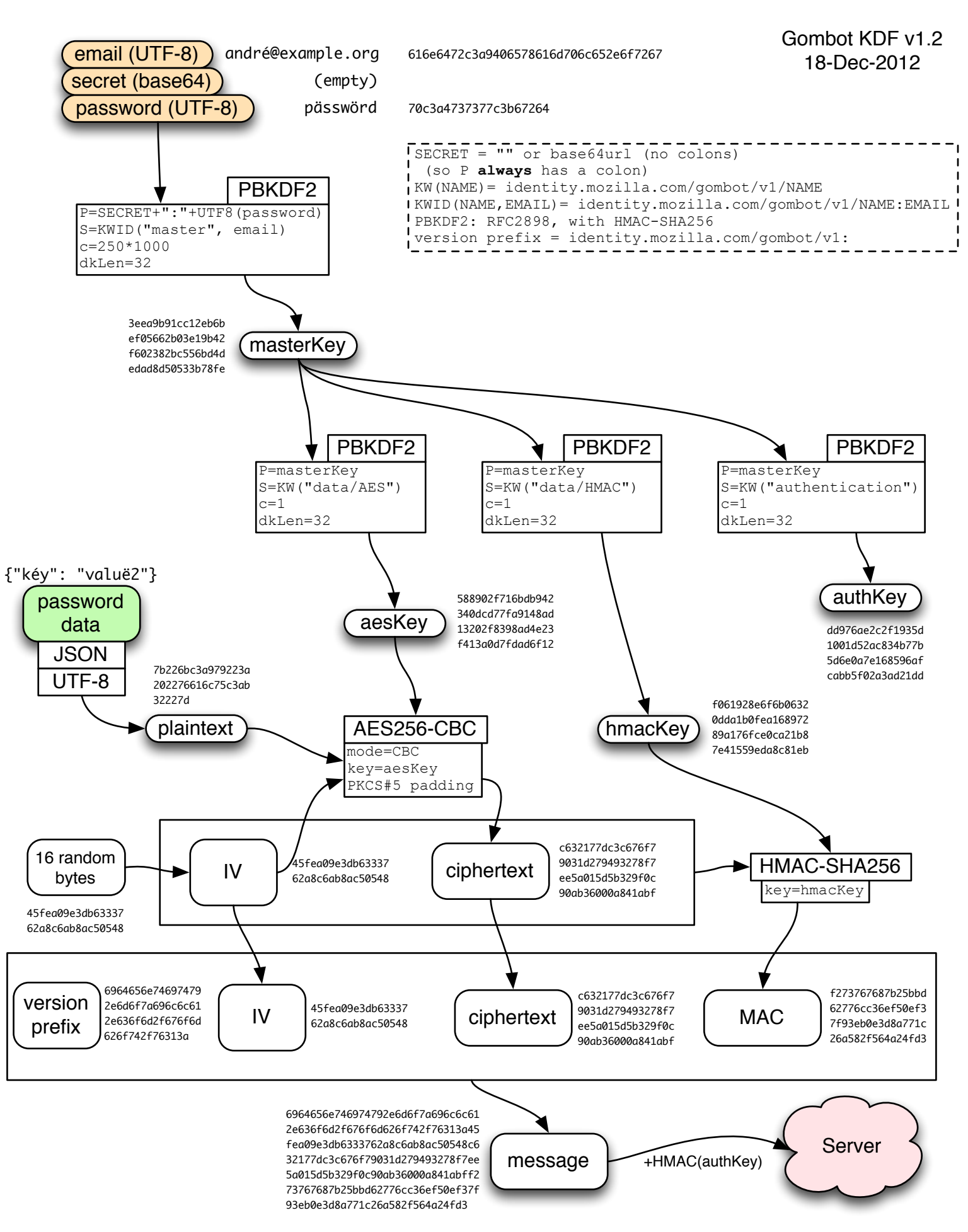
Gombot KDF v1.2
18-Dec-2012
email (UTF-8)
andré@example.org
616e6472c3a9406578616d706c652e6f7267
secret (base64)
(empty)
password (UTF-8)
pässwörd
70c3a4737377c3b67264
SECRET = "" or base64url (no colons)
(so P always has a colon)
KW(NAME)= identity.mozilla.com/gombot/v1/NAME
KWID(NAME,EMAIL)= identity.mozilla.com/gombot/v1/NAME:EMAIL
PBKDF2: RFC2898, with HMAC-SHA256
version prefix = identity.mozilla.com/gombot/v1:
PBKDF2
P=SECRET+":"+UTF8(password)
S=KWID("master", email)
c=250*1000
dkLen=32
3eea9b91cc12eb6b
ef05662b03e19b42
f602382bc556bd4d
edad8d50533b78fe
masterKey
PBKDF2
P=masterKey
S=KW("data/AES")
c=1
dkLen=32
PBKDF2
P=masterKey
S=KW("data/HMAC")
c=1
dkLen=32
PBKDF2
P=masterKey
S=KW("authentication")
c=1
dkLen=32
{"kéy": "valuë2"}
password data
JSON
UTF-8
7b226bc3a979223a
202276616c75c3ab
32227d
plaintext
aesKey
588902f716bdb942
340dcd77fa9148ad
13202f8398ad4e23
f413a0d7fdad6f12
authKey
dd976ae2c2f1935d
1001d52ac834b77b
5d6e0a7e168596af
cabb5f02a3ad21dd
AES256-CBC
mode=CBC
key=aesKey
PKCS#5 padding
hmacKey
f061928e6f6b0632
0dda1b0fea168972
89a176fce0ca21b8
7e41559eda8c81eb
16 random bytes
45fea09e3db63337
62a8c6ab8ac50548
IV
45fea09e3db63337
62a8c6ab8ac50548
ciphertext
c632177dc3c676f7
9031d279493278f7
ee5a015d5b329f0c
90ab36000a841abf
HMAC-SHA256
key=hmacKey
version prefix
6964656e74697479
2e6d6f7a696c6c61
2e636f6d2f676f6d
626f742f76313a
IV
45fea09e3db63337
62a8c6ab8ac50548
ciphertext
c632177dc3c676f7
9031d279493278f7
ee5a015d5b329f0c
90ab36000a841abf
MAC
f273767687b25bbd
62776cc36ef50ef3
7f93eb0e3d8a771c
26a582f564a24fd3
6964656e746974792e6d6f7a696c6c61
2e636f6d2f676f6d626f742f76313a45
fea09e3db6333762a8c6ab8ac50548c6
32177dc3c676f79031d279493278f7ee
5a015d5b329f0c90ab36000a841abff2
73767687b25bbd62776cc36ef50ef37f
93eb0e3d8a771c26a582f564a24fd3
message
+HMAC(authKey)
Server