SIP Authentication using EC-SRP5 Protocol

Fuwen Liu, liufuwen@chinamobile.com

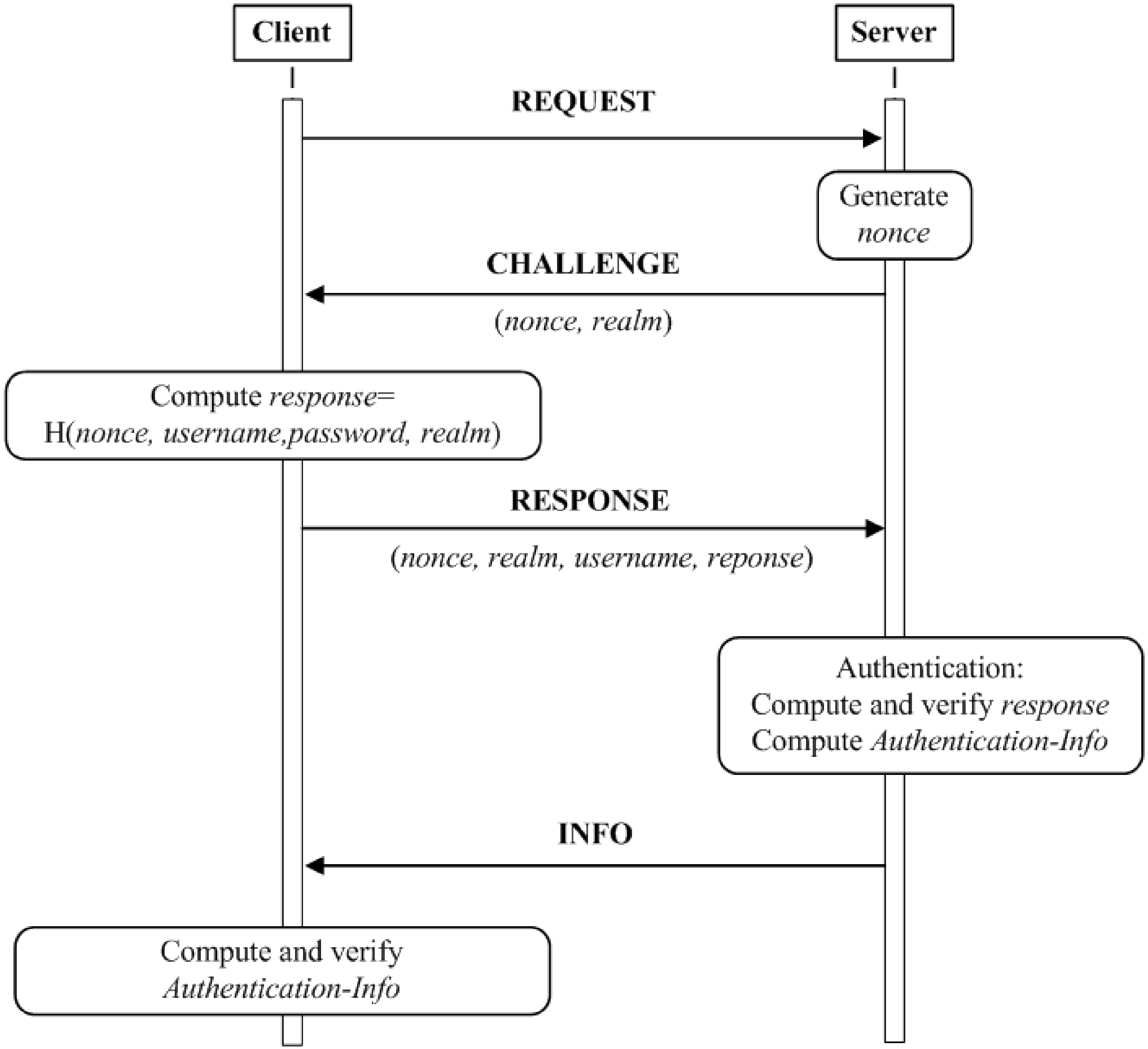
Minpeng Qi, qiminpeng@chinamobile.com

Min Zuo, zuomin@chinamobile.com

SIP Authentication

- SIP is a popular standard signaling protocol for VoIP
  - Wired networks
  - Wireless networks (3GPP)
- SIP applies HTTP digest authentication (RFC 2069 and RFC 2617) as one option for user authentication.

SIP Authentication based on HTTP digest



HTTP Digest Authentication

Client

Server

Query: GET/cgi-bin/checkout ?Cart=15672 HTTP/1.1

Challenge: realm, nonce, algorithms

Response: Hash(HA1, nonce, HA2)

Where: HA1=Hash (Username, realm, Passward)
HA2=Hash(Algorithms , DigistURI)

- **Breaking the scheme by computing**

Response $\stackrel{?}{=}$ hash(hash(Username,realm, ***guessed Password***), nonce, HA2)

Password Authentication

- **Password—one of special pre-shared key.**
  - Prove that an entity knows the password.
  - Pro: Easy to use, Low costs, Efficiency
  - Con: Low security
    - Password usually short, less than 8 characters
      - Machine randomly generated password from 88 printable characters
        - Security strength: $88^8 \approx 52$bits symmetric algorithms
          - 56 hours to crack (Special Hardware)
      - User-slected password from 88 printable characters (some combinations are i n dictionary)
        - Security strength: 30-bit strength
          - 16 minutes to crack (NIST)
    - Not scalable

Weaknesses of SIP Authentication

- Off-line dictionary attacks are possible
  - Select a password *pw`* from password dictionary and com pare:

$$H(nonce, username, pw`, realm) \stackrel{?}{=} response$$

Strong Password Authentication

- **In 2009, IEEE released the standard IEEE P1363.2 regarding the password authenticated k ey agreement protocols**
  - Balanced password-authenticated agreement protocols (BPKAS)
    - Two entities know the same password and establish a shared session key
    - well suited for P2P communications
    - Three protocols are recommended: PAK, PPK, SPEKE.
    - PAK is documented in RFC 5683 as standard
  - Augmented password-authenticated agreement protocols (APKAS)
    - Client knows the password, while the server knows only the image of the p assword
    - Well suited for client/server communications
    - Seven protocols are standardized, SRP(Secure Remote Password) protoc ol is one of representatives
    - SRP is specified in RFC 2945 by IETF

EC-SRP5 Protocol

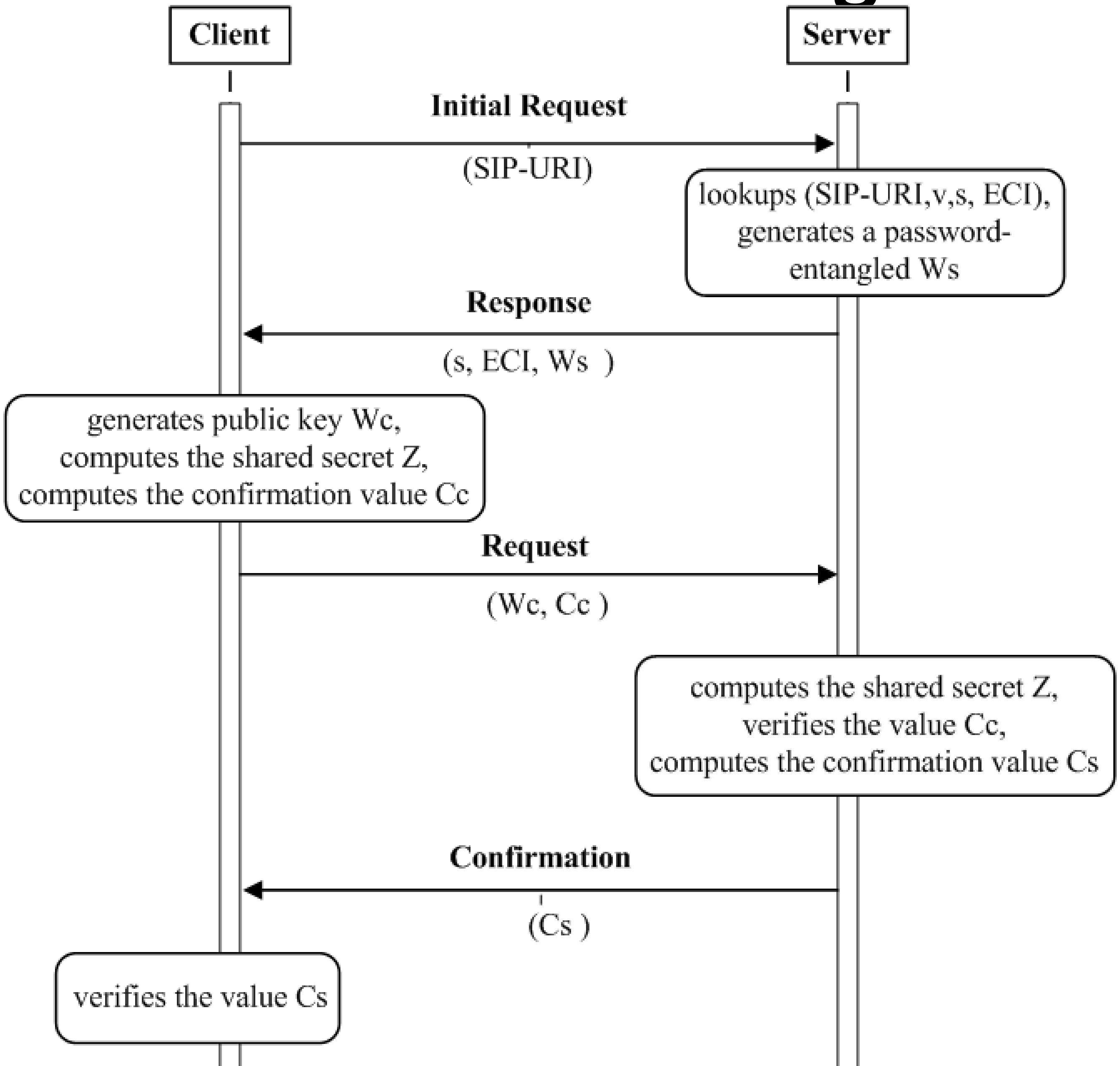
- EC-SRP5 protocol is an ECC variant of the SRP protocol
  - **Defined in IEEE 1363.2**
  - Authentication framework is identical to the SRP protocol
  - Using Elliptical Curve Cryptography
  - Security is based on the ECDLP problem
  - **More efficient than SRP protocol**
    - *ECC is used*
  - **Applying the EC-SRP5 protocol rather than the SRP protocol to SIP Aut hentication**
  - The basic idea of the EC-SRP5 protocol is that the password is entangled into the temporary EC public key
    - *To access the password, attackers have to address the ECDLP proble m*

Password verifier

- Password verifier v is computed:
  - i=OS2IP(SHA-256(s|SHA-256(SIP-URI|":"|Pw|ECI)))
  - v=i*G
    - where OS2IP means octet string to integer conversion primitive, the
    - derived password verifier v is actually a point on the elliptic curve
    - indicated by the ECI.

- The server then stores the following information in the data base for each user
  - SIP-URI
  - salt s
  - elliptic curve index ECI
  - password verifier v

SIP Authentication using EC-SRP5



Security Considerations

- Off-line dictionary attack resistance
  - Password-entangled public key Ws is available to attackers
    - *Ws=Ts*G+e1*
    - Where Ts is the temporary private key of server
  - Password verifier is used as input selector value to choose a pseudo-random element e1 of a group
  - The element e1 is shadowed by adding the point Ts*G.

- On-line dictionary attack resistance
  - The server usually blocks the user authentication
    - *when the times of authentication failure reach the default value set in advance.*

Security Considerations(cont'd)

- Man-in-the middle attack resistance
  - Verifying the confirmation value Cc and Cs in the client's side and server's side, respectively.

    Cc=SHA-256(hex(04), Wc, Ws, Z, v)

    Cs=SHA-256 (hex(03), Wc, Ws, Z,v)

- Replay attack resistance
  - Each authentication session has its unique shared secret Z
  - The client can detect the replay attack by comparing Cs with the expected confirmation value Cs'

Elliptic Curve Index

Description	ECI
secp224k1	1.3.132.0.32
secp224r1	1.3.132.0.33
secp256k1	1.3.132.0.10
secp256r1	1.2.840.10045.3.1.7
secp384r1	1.3.132.0.34
secp521k1	1.3.132.0.35
brainpoolP256r1	1.3.132.0.26
brainpoolP384r1	1.3.132.0.27
brainpoolP512r1	1.3.132.0.28

Thanks

Appendix A: Algorithm ECPEPKGP-SRP5-SERVER

- The following steps are needed to compute the elliptic curve password-entangled public key Ws:

(1) Compute octet string o1=GE2OSP-X(v)
(2) Compute group element e1=ECREDP(o1)
(3) Compute group element Ws=Ts*G+e1
(4) Output Ws as the password-entangled public key

Where GE2OSP-X is used to convert group elements into octet strings. ECREDP is Elliptic Curve Random Element Derivation Primitive

Appendix B: Algorithm ECSVDP-SRP5-CLIENT

- The following steps are needed to compute the shared secret value Z in client:

  (1) Compute octet string o1=GE2OSP-X(Wc)
  (2) Compute octet string o2=GE2OSP-X(Ws)
  (3) Compute octet string o3=SHA-256(o1|o2)
  (4) compute an integer i2=OS2IP(o3)
  (5) Compute octet string o4=GE2OSP-X(v)
  (6) Compute group element e1=ECREDP(o4)
  (7) Compute group element e2=Ws-e1
  (8) Compute i3=OS2IP(SHA-256(s|SHA-256(SIP-URI|":"|Pw|ECI)))
  (9) Compute group element zg= (Tc+(i2.i3))*e2
  (10) Compute field element z= GE2SVFEP (zg)
  (11) Compute shared secret value Z=FE2OSP (z)
  (12) Output Z

Where GE2SVFEP is the primitive for group element to secret value field element conversion, FE2OSP is field element to octet string conversion primitive. Tc is the temporary private key of client

Appendix C: Algorithm ECSDVP-SRP5-SERVER

- The following steps are needed to compute the shared secret value Z in server:

(1) Compute octet string o1=GE2OSP-X(Wc)
(2) Compute octet string o2=GE2OSP-X(Ws)
(3) Compute octet string o3=SHA-256(o1|o2)
(4) compute an integer i2=OS2IP(o3)
(5) Compute group element zg= Ts*(Wc+i2*v))
(6) Compute field element z= GE2SVFEP (zg)
(7) Compute shared secret value Z=FE2OSP (z)
(8) Output Z

Appendix D: Computing Wc

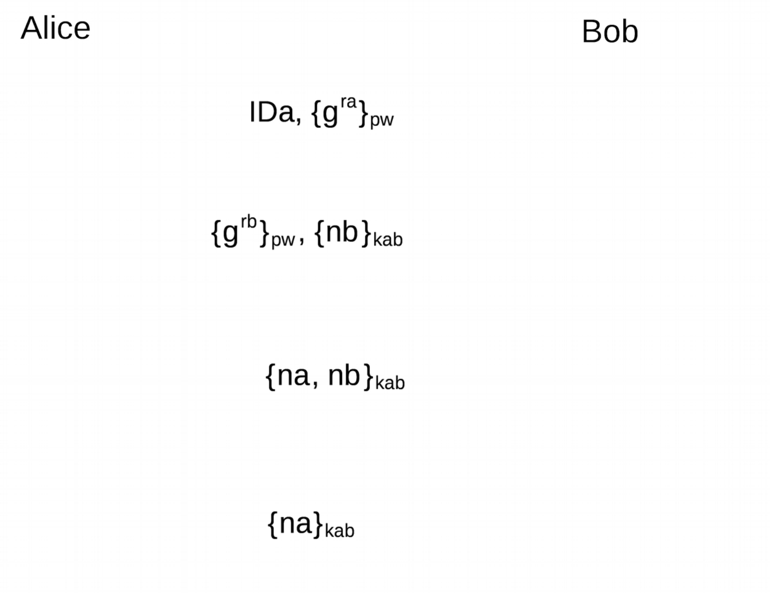
- The public key of client Wc is computed:

$$Wc = Tc*G$$

Where Tc is the temporary private key of client

Encrypted key exchange-DH(EKE-DH)

- **1992, Bellovin invented EKE-DH to address this problem first. Its procedure is:**
  - Alice sends its identity *IDa* and DH-public key g^{r_a} encrypted with password *Pw* to Bob
  - Bob encrypts its DH-public key g^{r_b} with password *Pw*, and generates a shared $Kab=g^{r_a r_b}$. The nonce *nb* is protected by *Kab*.
  - Alice generates the shared *Kab*, and decrypts $\{nb\}_{Kab}$, and encrypts its nonce *nb* as well as *nb* with *Kab.*
  - Bob decrypts $\{na,nb\}_{Kab.}$ If the decrypted *nb* is identical to the *nb* it sended, the Alice is authenticated.
  - Alice decrypts $\{na\}_{Kab.}$ If the decrypted *na* is identical to the *na* it sended, the Bob is authenticated.



Variants of EKE-DH

- **The key point of EKE-DH is that ephemeral public DH keys are encrypted with the password.**
  - Unable to mount off-line dictionary attacks
    - Public DH keys are random strings
  - Unable to discover the session key
    - Private DH keys are unknown to attacks

- **The basic idea to combine asymmetric algorithms with symmetric algorithms to foil the off-line dictionary attacks has been extended. This can be abstracted as public DH keys are entangled by using the password. This leads to**
  - PAK (Password Authenticated key exchange) and PPK (Password Protected Key exchange)
    - Password-entangled DH public key is: $f(Pw).g^x \bmod p$
  - SPEKE (Secure Password Exponential key Exchange)
    - Password-entangled DH public key is: $f(Pw)^x \bmod p$

Standards and Patents

Protocols	Security analysis	IEEE P1363.2	RFC	Patents
EKE-DH	Several papers	--	--	US and EU patents
PAK	Provely secure	Yes	Yes	Patent held by Lucent
PPK	Provely secure	Yes	No	Patent held by Lucent
SPEKE	Provely secure	Yes	No	Phoenix held the patent
SRP	Provely secure	Yes	Yes	Standford Uni held the patent, license free
EC-SRP5	--	Yes	No	No

- **IEEE takes no position with respect to the existence of validity of any patent rights.**
- **In RFC, usually a patent-free scheme is easy to become a standard, but a patented scheme may be standardized if no patent-free scheme can replace it.**

Operation of EC- SRP5 protocol

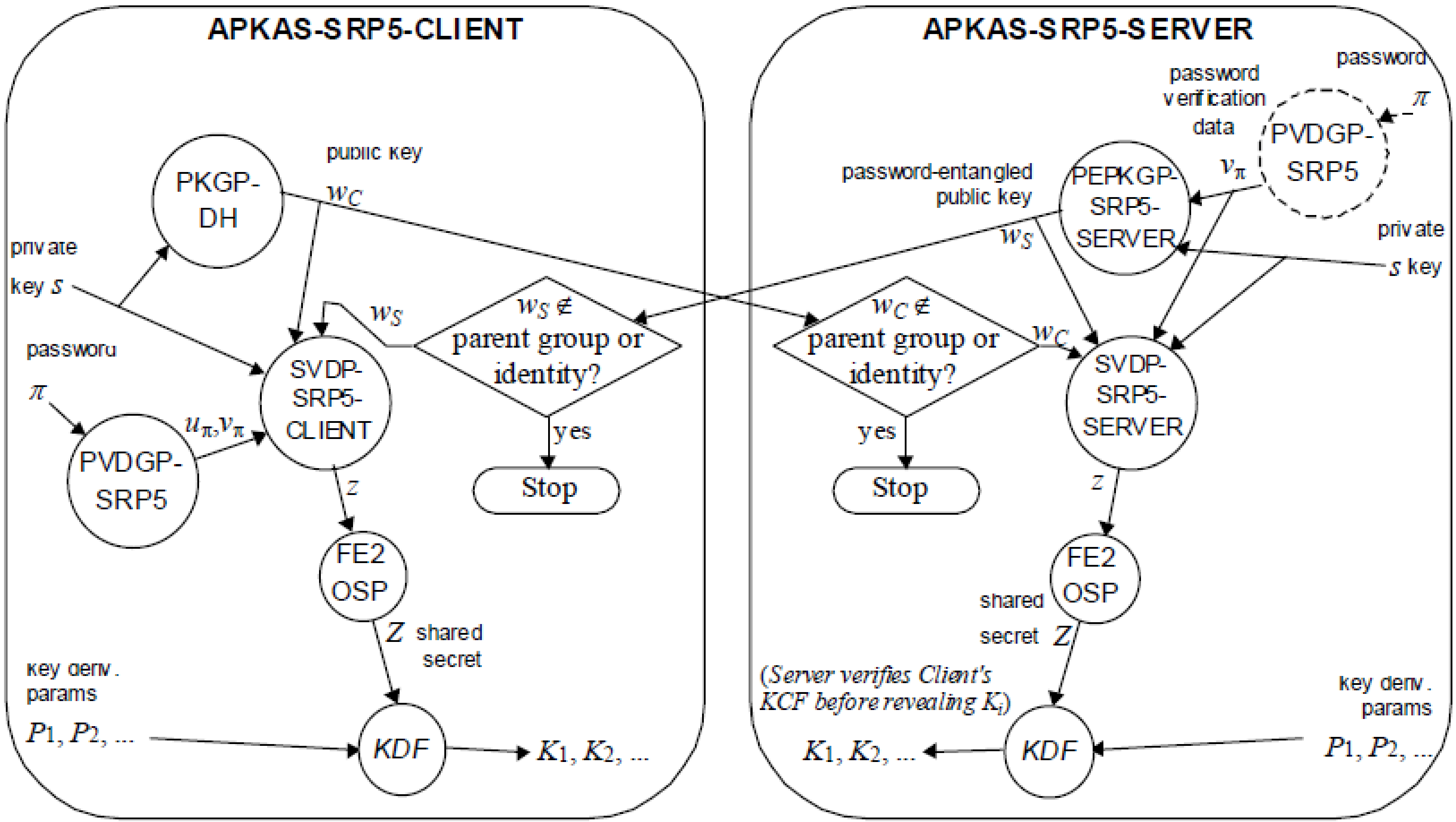


Figure 10—APKAS-SRP5 key agreement operation

Terms

ECI: elliptic curve index
G: a base point (xG, yG) on an elliptic curve
s:salt
Tc: client's temporary private key
Ts: server's temporary private key
Wc: client's public key
Ws: server's public key
Cc: client's confirmation value
Cs: server's confirmation value
Pw: password
v: password verifier
Z: shared secret between client and server
SIP-URI: Uniform Resource Identifier for SIP
containing user name and domain name
The | symbol denotes string concatenation,
the * operator is the scalar point multiplication operation in an EC group
the . operator is the integer multiplication.
ECDLP: Elliptic Curve Discrete Logarithm Problem

Authentication methods

- **Digital signatures**
  - Prove that an entity has the private key used for signatures
  - Pro:
    - Scalability
    - Easy to use
    - High security
      - E.g, the key length of the private key is usually about 2048 bits, which corresponds to 112 bits key length of the symmetric algorithms.
  - Con: PKI required
    - High costs
    - Expensive management

Authentication methods

- **Pre-shared key**
  - Prove that an entity knows the pre-shared key
  - Pro: Low costs
  - Con:
    - Difficult to use
      - For security, the pre-shared key is required to be generated randomly, and its key length requires 64 bytes, as specified in IKEv2
    - Not scalable
      - Pre-shared keys can be only distributed to the known partners