A Signature Based Mutual Authentication Protocol for Remote Health Monitoring

Ms. Sumitra Binu

Asst. Professor

CHRIST
(Deemed to be University)

Dr. Mohammed Misbahuddin

Joint Director

ACTS & BD
C-DAC
(Bangalore)

Mr. Joy Paulose

Associate Professor

CHRIST
(Deemed to be University)

INTERNATIONAL CONFERENCE ON INTERNET RESEARCH AND ENGINEERING (ICIRE 2019)

5/3/2019

Contents

- Introduction
- Related Work
- Proposed Scheme
- Security Analysis
- Formal Analysis
- Efficiency Analysis
- Conclusion

Introduction

- In 2008 , the number of aging people world wide was estimated at 506 million and in 2040, number will touch 1.3 billion.[1]
- 7 Million patients in India need Palliative Care every year[2]
- In India Health care resources are heavily urban biased.
- Country faces a humungous resource gap of over 4 million health workers.[3]

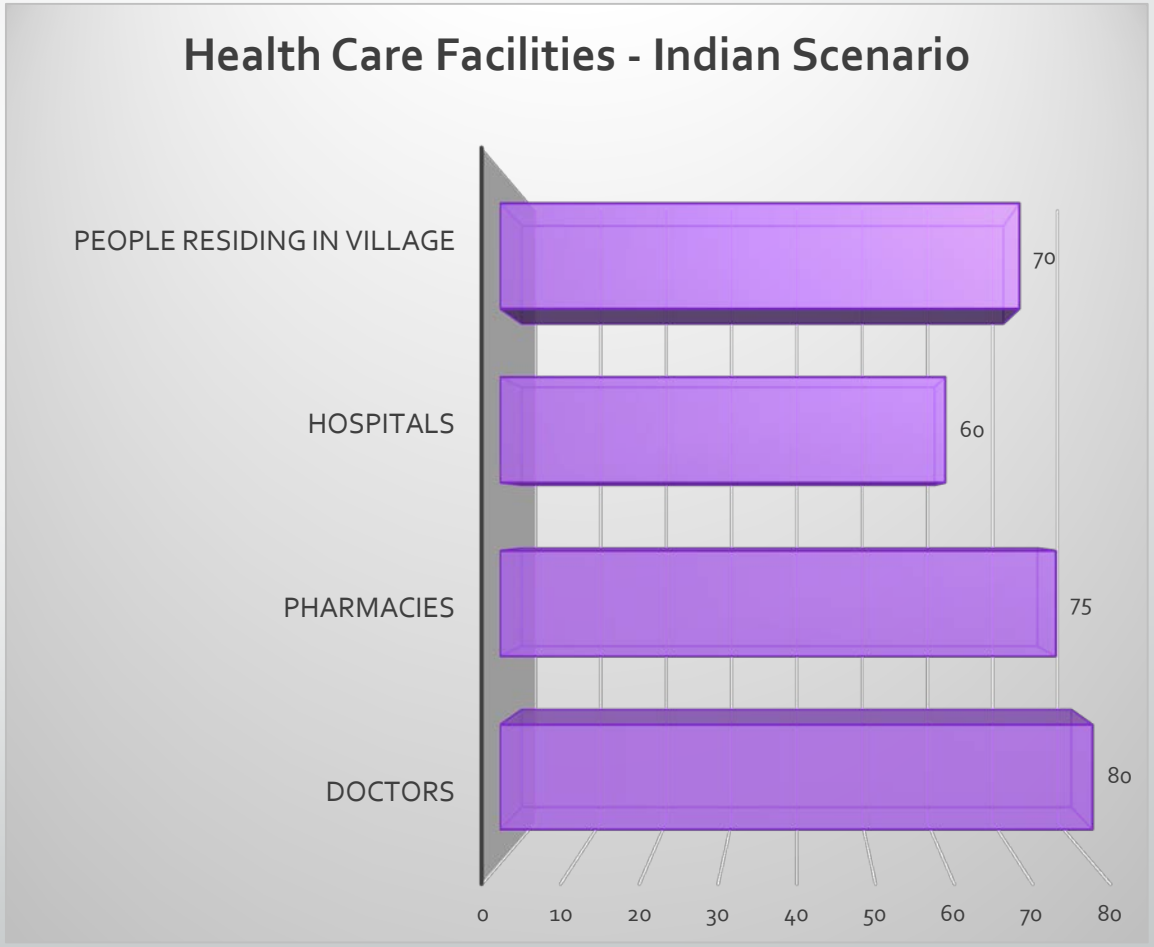


Fig. 1 source: India's Most Villages Are Getting Better Health Care With. This Cloud Based Solution [3,4]

Introduction

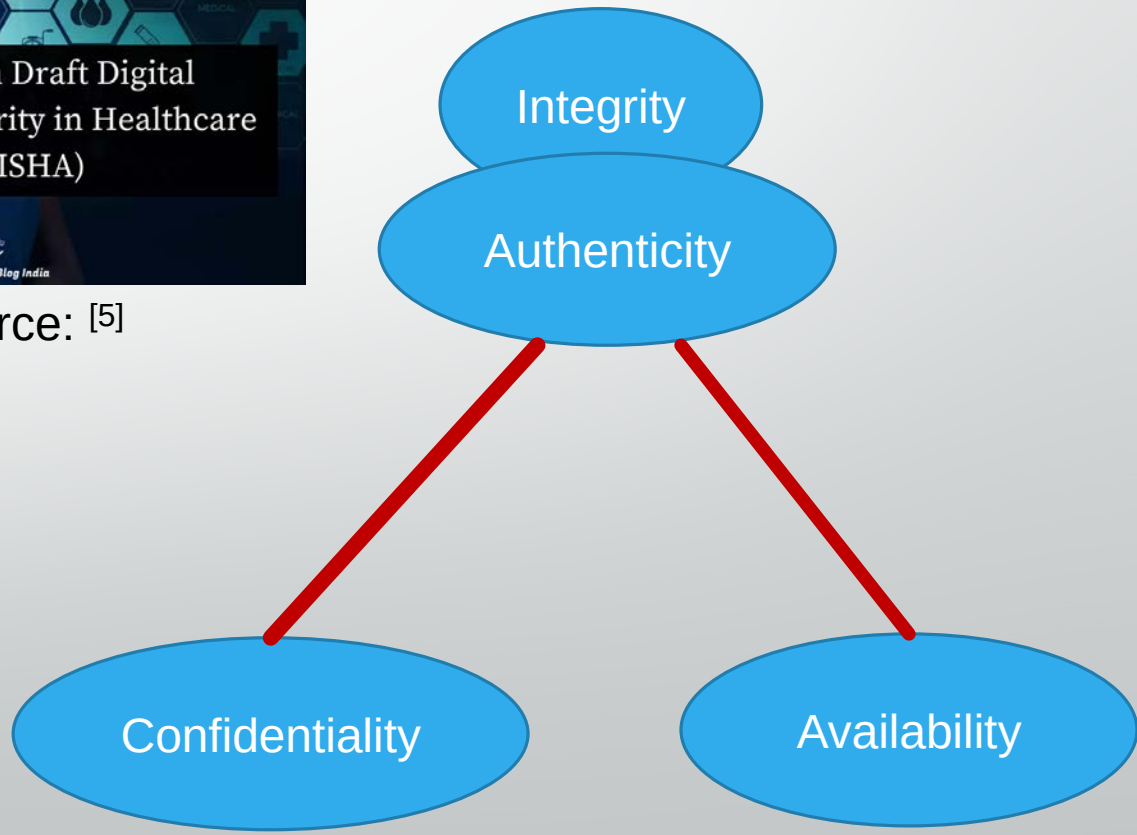
- Ubiquitous health Monitoring drastically reduces hospital visits
- Portea, Zoctr, Health Care at Home , Care24 etc. provides health care services at home.
- IOMT sensors adds life on to the days of patients enjoying the comforts of home.
- WBAN Sensor devices and mobile devices enable continuous remote monitoring of vital signs .

Challenges

- Many medical devices tracking health care data run on public networks.
- No regulations to ensure secure management of sensitive data[5].
- Concerns: Security & Privacy

Fig. 2 source: [6]

Fig. 3 source: [5]



Focus: A Secure Authentication Mechanism

Related Work

Year	Proposed By	Methodology	Observations
2011	Yeh et al.[7]	ECC	Fails to Provide Mutual Authentication, Computationally Complex
2012	Kumar et al. [8]	Symmetric Key Key Cryptography	Fails to provide user anonymity, susceptible to to privileged insider attack & offline password password guessing attack
2013	Shi and Gong[9]	ECC	Computationally Intensive, Need more memory memory to store sensor nodes & user's public public key values
2015	Hi et al. [10]	Hash Functions	Error in detection of wrong password, incorrect incorrect approach for key establishment, Susceptible to DOS
2015	Li et al. [11]	Symmetric Key	Susceptible to sensor node capture attack &

Proposed Scheme - Participants

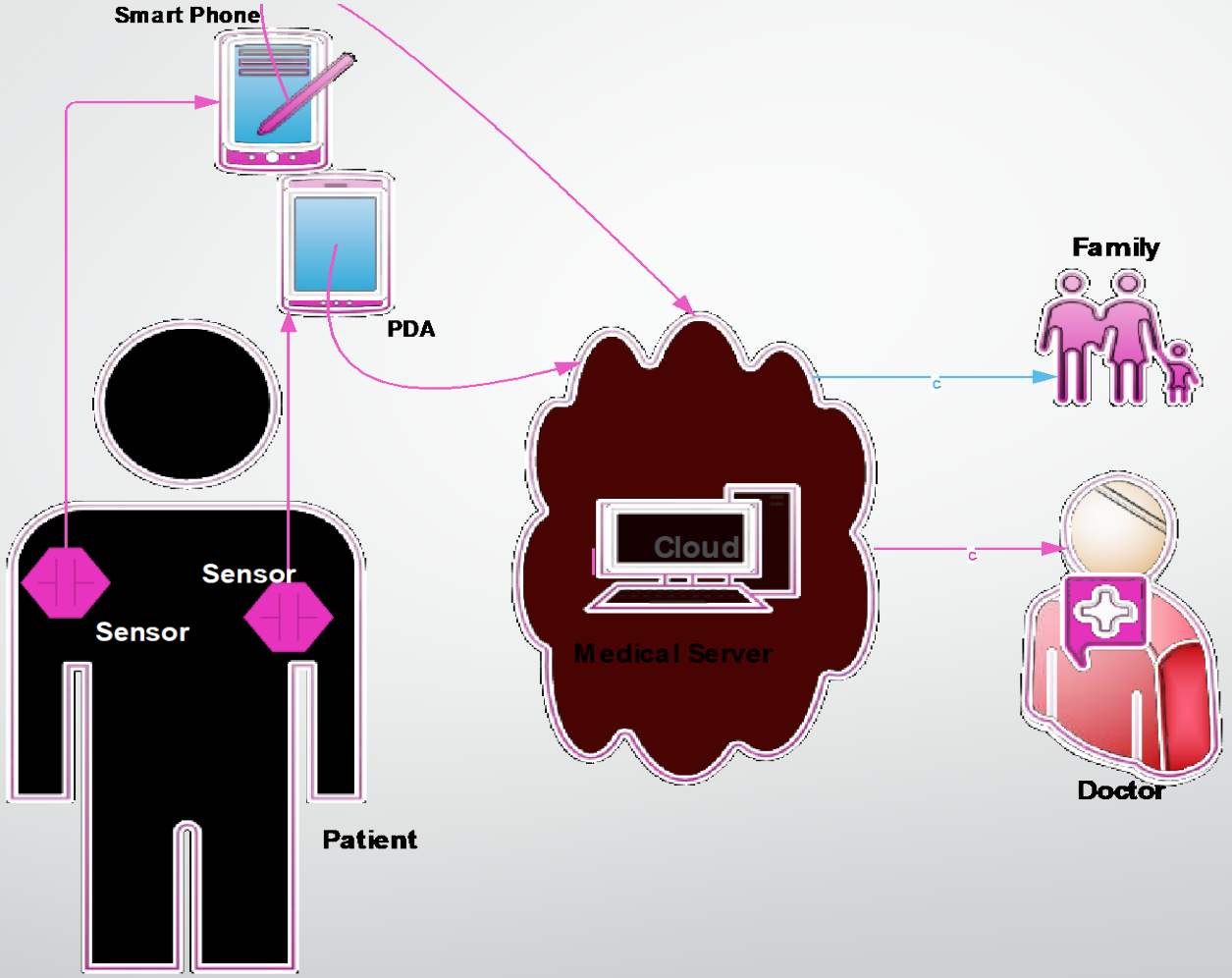
Sensors

Personal Devices

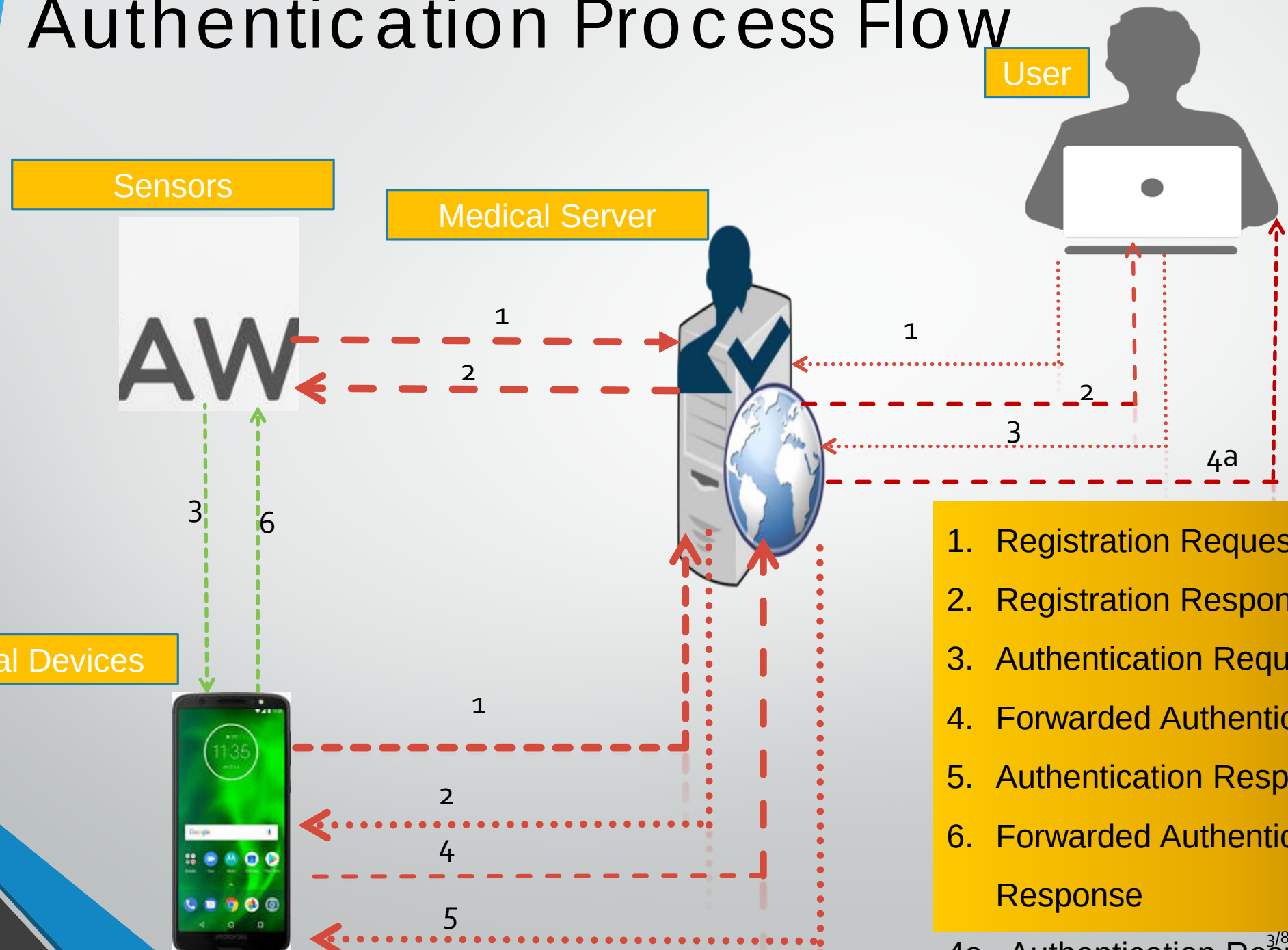
Medical Server

User

PROPOSED ARCHITECTURE



Authentication Process Flow



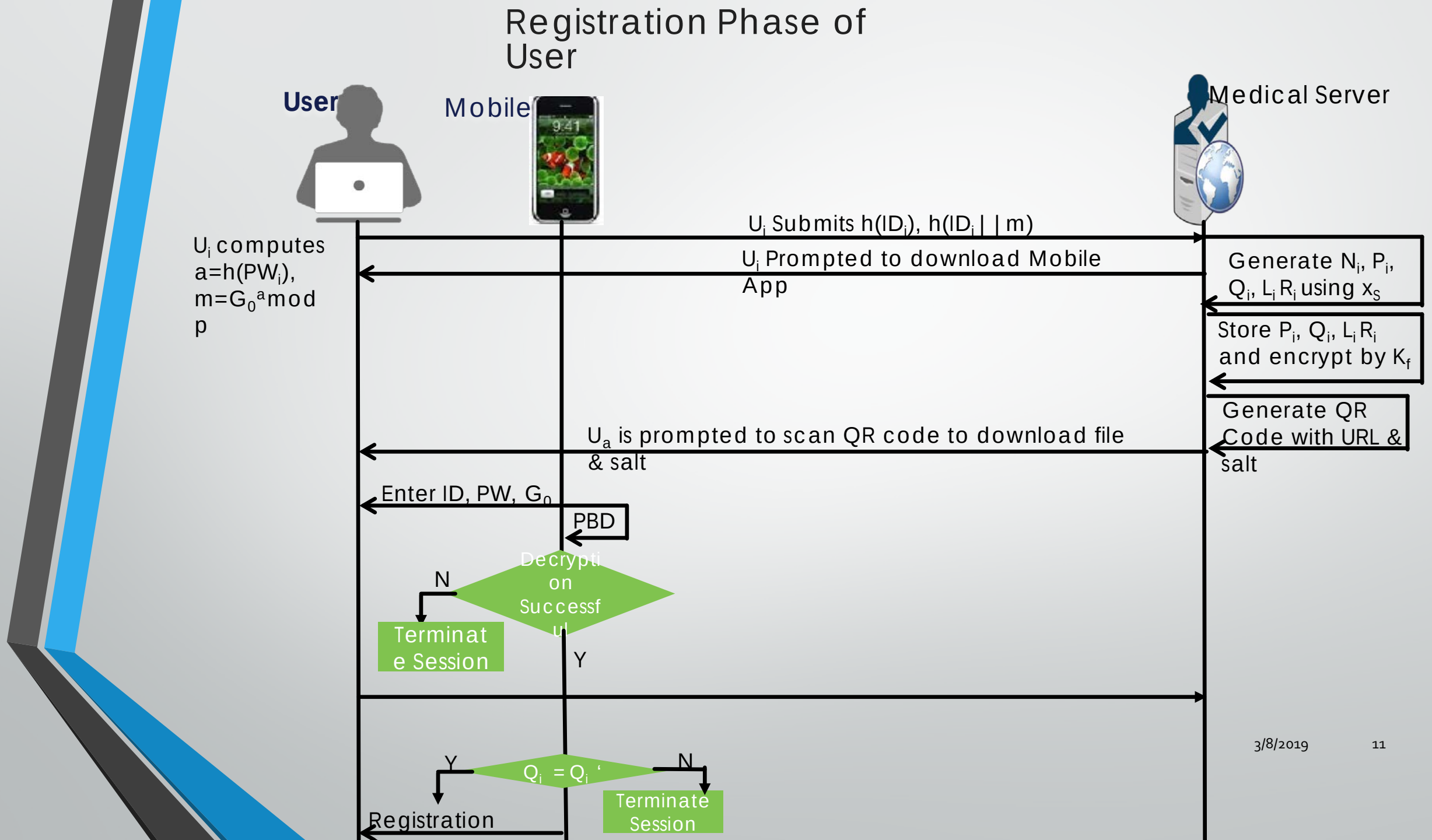
1. Registration Request
2. Registration Response
3. Authentication Request
4. Forwarded Authentication Request
5. Authentication Response
6. Forwarded Authentication Response

Notations

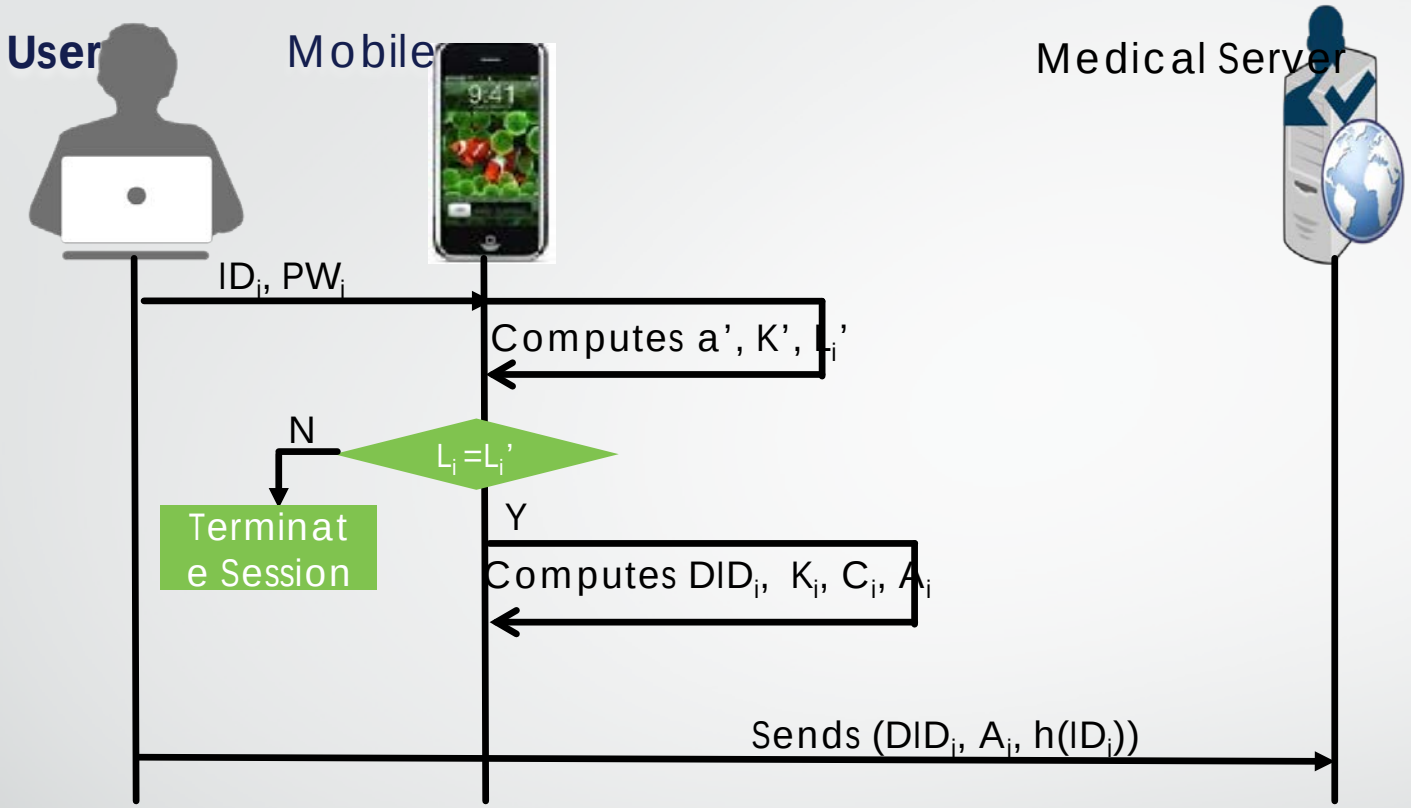
Table 1. Notations Used

ID_i, PW_i, SID_i, PID_i, ID_{MS}	**Identity, Password of user U_i, ID of Sensor, ID of PD, ID of Medical Server**
x_s, K_{ps}, K_{ws}	Secret key of Server, Key of PD, Key of Sensor
P , G_0	Prime number, generator of cyclic group
Salt	Pseudorandom value
h(.) , ⊕ , ‖	hash function, XOR , Concatenation
N_1, N_2, C_1, C_2, C_3	Nonce Values

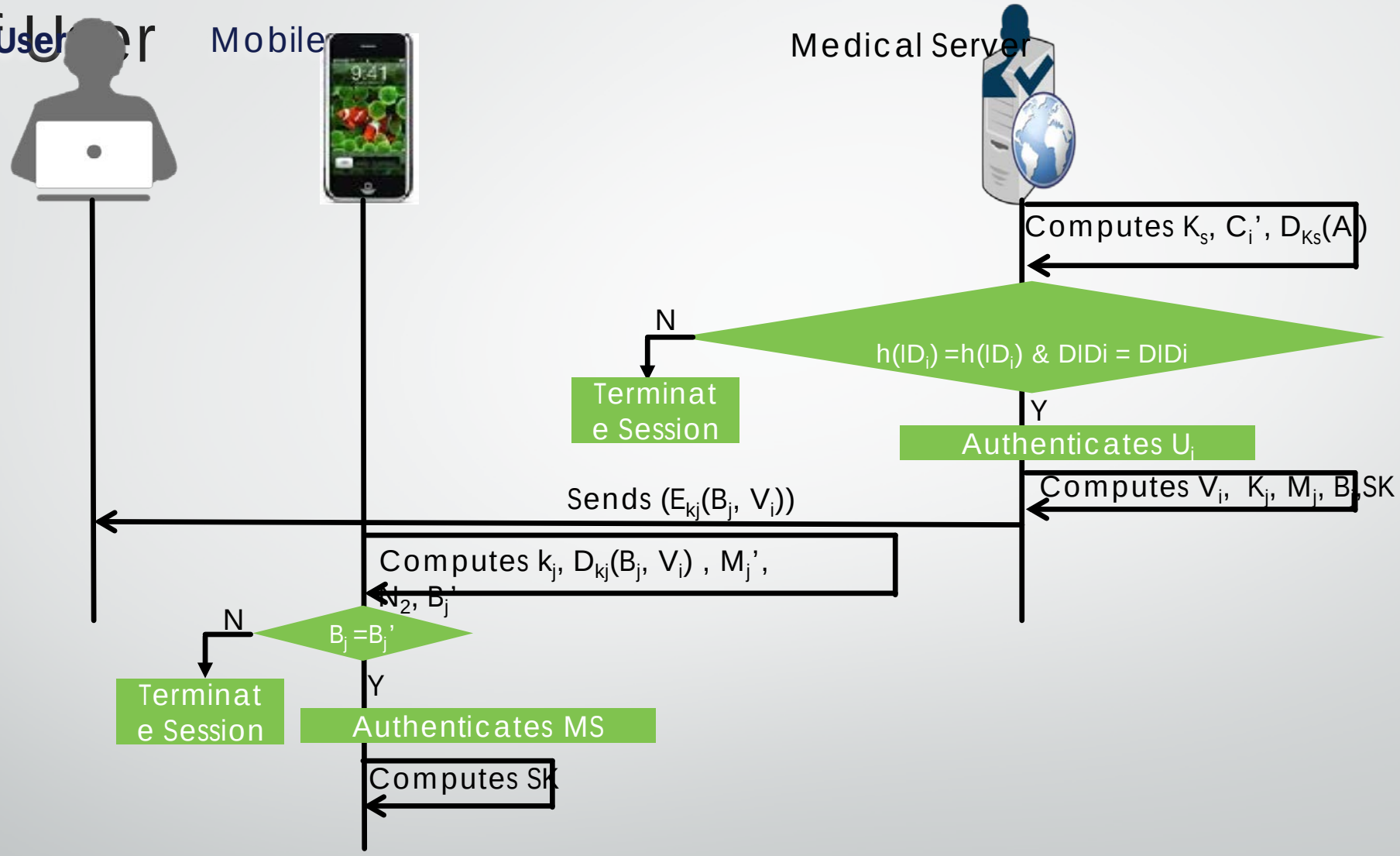
Registration Phase of User



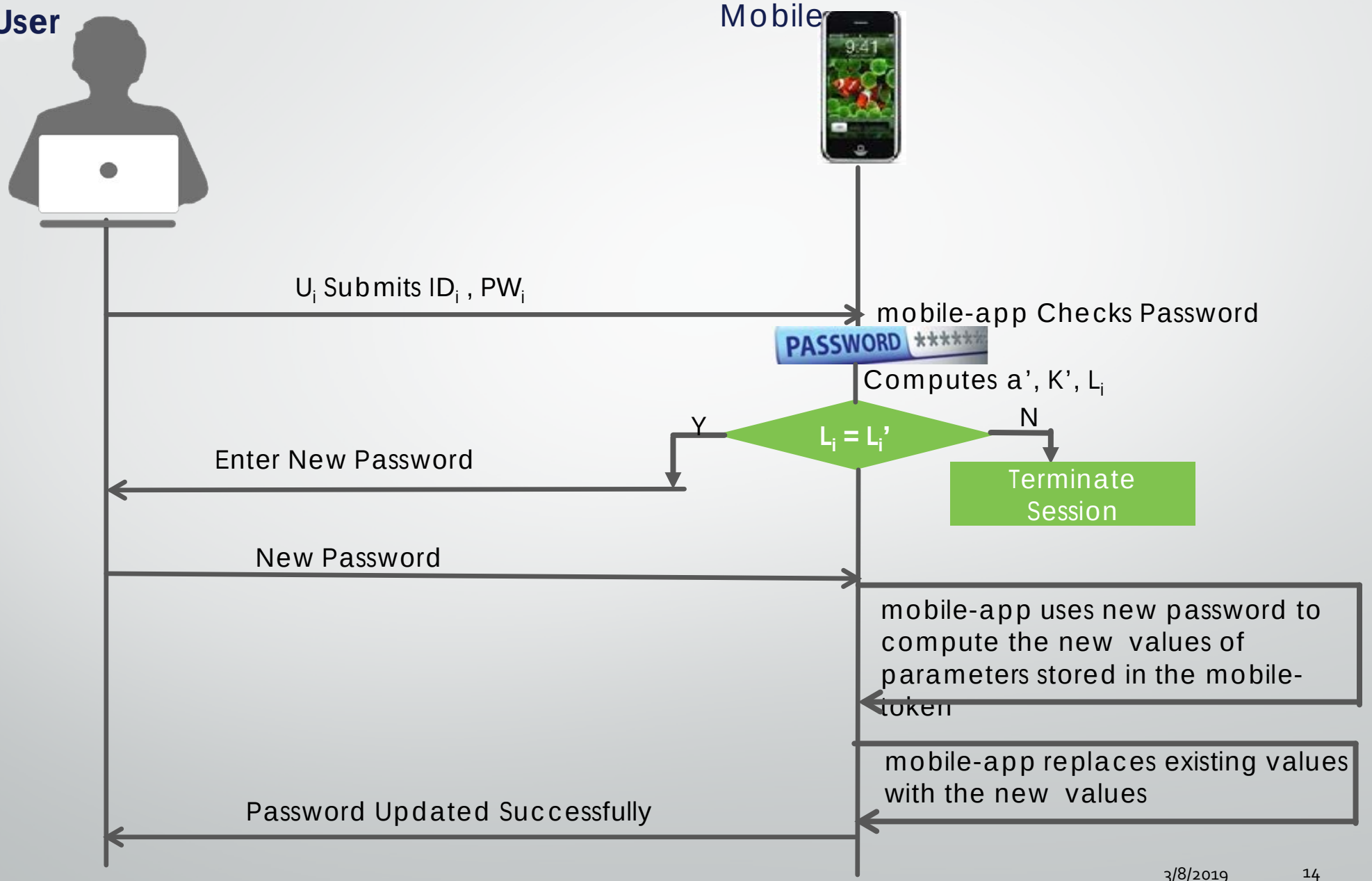
Login Phase of User



Authentication and Key Agreement Phase of User



Password Change Phase



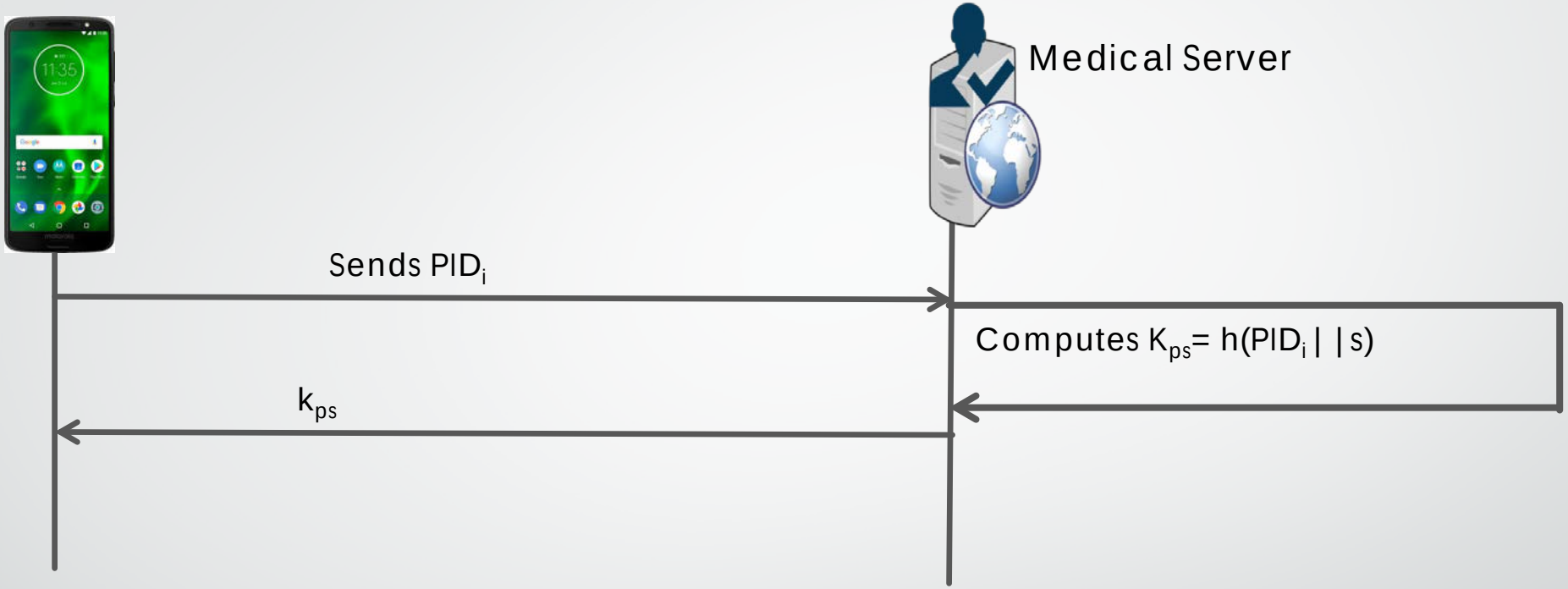
Initialization Phase of Medical Server

Global Public key:
p ,q, a
P & q are prime; $a^q = 1 \bmod p$

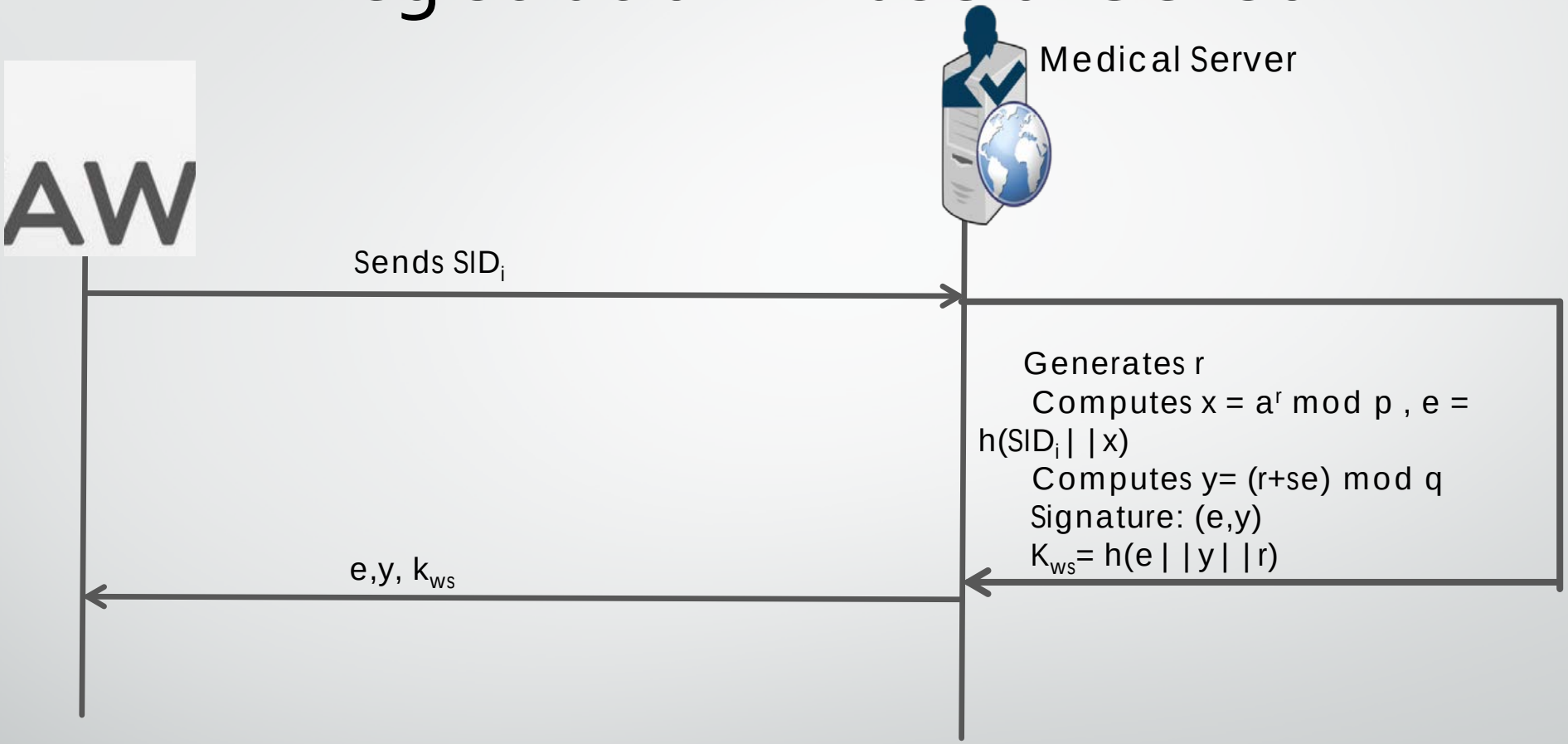
Private Key: s
o <s<q

Public Key of Medical Server:
$V = a^{-s} \bmod q$

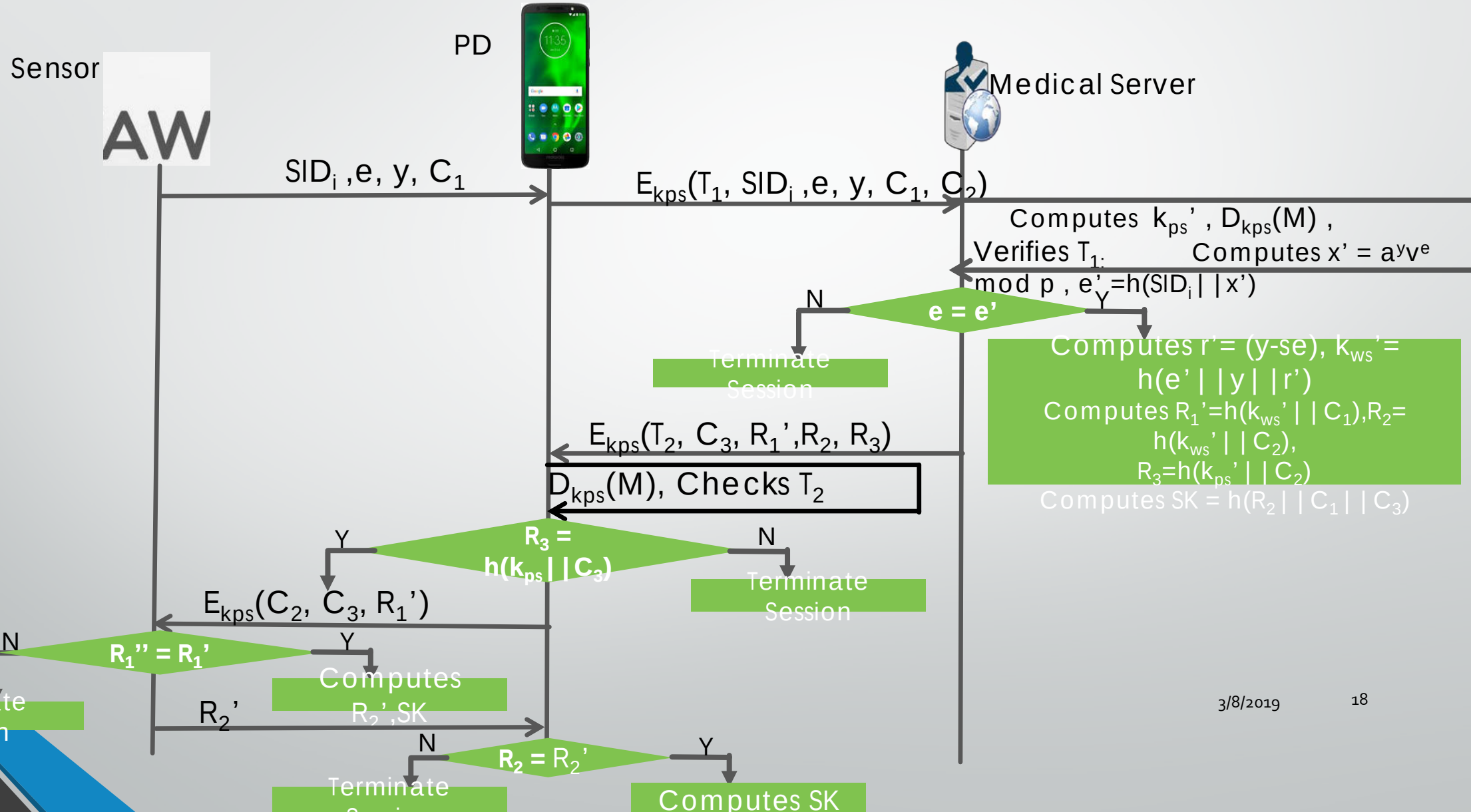
Registration Phase of Personal Device



Registration Phase of Sensor



Authentication & Key Agreement Phase of Sensor, Personal Device and Medical Server



Security Analysis

- Security Properties
  - Patient Anonymity
  - Mutual Authentication
    - Case 1: Mutual Authentication of User and Medical Server
    - Case 2: : Mutual Authentication of Sensor, Personal Device and Medical Server

- Resistance to Common Attacks
  - Impersonation Attack
    - Case 1: An attacker with malicious intentions fakes to be a sensor node and transmits wrong information
    - Case 2: An attacker with malicious intentions fakes to be a PD and transmits wrong information
    - Case 3: An attacker with malicious intentions fakes to be a MS and transmits wrong information
    - Case 4: A malicious user pretends to be an authorized user and attempts to access sensitive data

Security Analysis

- Resistance to Common Attacks
  - Medical Server Spoofing Attack
  - Replay Attack
  - Privileged Administrator Resilience Attack
  - Stolen Verifier Attack
  - Malicious Insider Attack
  - Modification Attack
  - Man-in-the-Middle Attack

Formal Analysis – Scyther Tool

- Scyther
  - An automated formal verification tool used to guarantee the security of a protocol [12]
  - Requires creation of a mathematical model of the protocol and a network which is assumed to be under full control of the adversary [13]
  - Scyther provides a graphical user interface incorporating the Scyther command line and python scripting interface.
- The description of a protocol and the claims in Scyther are written in Security Protocol Description Language (SPDL).
- Formal Semantics of Scyther:
  - Roles: Distinct behaviors of the protocol and defined by a sequence of events
  - Agents: Agents perform one or more roles
  - Run: An instance of a protocol role
  - Events:
    - **Send and recv events :** Marks sending and receiving a message
    - **Claim events :** Used in role specifications to model intended security properties

Proposed Protocol in SPDL

// Mutual Authentication Protocol for User and Medical Server
const exp: Function; hashfunction h; const XOR: Function;
const Fresh:Function;
protocol WSNUserLogin(I,R){
role I{
const ID_i,PW_i,X_s,mg1,mg2,p,g; macro k = mod(exp(g,h(PWi)),p); macro Li= (h(IDi),h(IDi,k));
macro DID_i = h(h(ID_i),N1,L_i);macro Ki=h(DIDi,C1); macro Ai=(DIDi,h(IDI), N1)ki;
macro Bj=h(DIDI,Mi,N2); macro C2=XOR(C1,N1,N2); macro Ki =h(DIDi, N1, C1);
send_1(I,R, DID_i, A_i,h(ID_i)); //Sending Login Reques
recv_2(R,I, {Bj,C2}kj); //receiving B_j and C_2
claim_i1(I,Secret, Ki); // claim ki
claim_i2(I, Secret, g);//claim for g
claim_i3(I, Alive); claim_i4(I,Niagree); claim_i5(I,Nisynch);
}

role R{
const IDi,PWi, p,g,Xs;
recv_1(I,R,DIDi,Ai, h(IDi)); //Receving Login Request
send_2(R,I, {Bj,C2}Kj); //Sending B_j and C_2
claim_r1(R,Secret,IDi); claim_r2(R,Secret, PWi); claim_r3(R, Niagree);
claim_r4(R,Nisynch); claim_r5(R,Alive);}
}

Initial Knowledge

Agents

Event

Claim

Roles

Claims

- Secrecy
  - Protocol ensures confidentiality of authentication parameters
  - The authentication paramèters {K_{ws}, K_{ps}, R_1,R_2, C_3,SK} retain the confidentiality during the course of Protocol runs.
- Non-Injective Agreement
  - Sender and receiver agree upon the values exchanged
  - Analysis results prove that the transmitted and received values are the same
- Non-Injective Synchronisation
  - Corresponding send and receive events occur in the correct order and have the same contents
  - Scyther analysis results prove that the claim is satisfied

Scyther Analysis - Results

auththree	I	auththree,i1	Secret C1	Ok	No attacks within bounds.
		auththree,i2	Secret s	Ok	No attacks within bounds.
		auththree,i6	Secret h(h(SIDi,mod(exp(a,r),p)),mod(add(r,mul(s,h...	Ok	No attacks within bounds.
		auththree,i3	Nisynch	Ok	No attacks within bounds.
		auththree,i4	Niagree	Ok	No attacks within bounds.
		auththree,i5	Alive	Ok	No attacks within bounds.
	R	auththree,r1	Secret C2	Ok	No attacks within bounds.
		auththree,R4	Secret h(h(h(SIDi,mod(mul(exp(a,mod(add(r,mul(s,h(...	Ok	No attacks within bounds.
		auththree,r2	Secret h(h(h(SIDi,mod(mul(exp(a,mod(add(r,mul(s,h(...	Ok	No attacks within bounds.
		auththree,r3	Secret h(h(PIDi,s),C3)	Ok	No attacks within bounds.
		auththree,r4	Secret h(PIDi,s)	Ok	No attacks within bounds.
	S	auththree,s1	Secret C3	Ok	No attacks within bounds.
		auththree,s2	Secret h(h(h(SIDi,mod(mul(exp(a,mod(add(r,mul(s,h(...	Ok	No attacks within bounds.
		auththree,s3	Secret h(h(h(SIDi,mod(mul(exp(a,mod(add(r,mul(s,h(...	Ok	No attacks within bounds.
		auththree,s4	Secret h(h(PIDi,s),C3)	Ok	No attacks within bounds.
		auththree,s5	Secret h(h(h(h(SIDi,mod(mul(exp(a,mod(add(r,mul(s,...	Ok	No attacks within bounds.
		auththree,s6	Secret h(h(SIDi,mod(exp(a,r),p)),mod(add(r,mul(s,h...	Ok	No attacks within bounds.
		auththree,s7	Secret h(PIDi,s)	Ok	No attacks within bounds.

Done.

Efficiency Analysis

Phases	Participant	Das's scheme [14]	Khan & Alghathbar [15]	Vaidya et al.[16]	Proposed scheme
Registration	U_i	0	1H	1H	7H+1X
	MS	3H+1X	2H+1X	4H+3X	5H+4X+3H
	S_i	0	0	0	0
	PD	-	-	-	0
Login	U_i	3H+1X	3H+1X	6H+4X	5H+1X
	MS	0	0	0	-
	S_i	0	0	0	-
	PD	-	-	-	-
Authentication& Key Agreement	U_i	0	0	1H+3X	4H+2X
	MS	4H+2X	5H+2X	6H+6X	7H+3X+7H
	S_i	1H	2H	2H+2X	3H
	PD	-	-	-	2H
Password Change	U_i	-	3H+2X	8H+6X	6H+4X
Total		11H+4X	16H+6X	28H+24X	59H+15X

Conclusion

- Advancements in WSN technologies have contributed to commendable development of sensor network applications.
- Remote Health Monitoring can address issues pertaining to lack of health care facilities and can reduce health care expenses
- WSNs play a promising role in Remote Health Monitoring and authentication of entities in a sensor network is a challenging concern
- This research proposed an authentication scheme for authenticating entities in WBAN
- Usability of proposed scheme is verified by carrying out security and efficiency analysis
- Formal Analysis is done using Scyther tool and results demonstrate that the protocol is resistant to various attacks.

References

1. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3279202/
2. https://caravanmagazine.in/perspectives/last-resort-india-palliative-care
3. Suparna D, “India’s Most Remote Villages are Getting Better Health Care with This Cloud Based Solution,” https://www.forbes.com/sites/suparnadutt/2016/11/21/indias-most-remote-villages-are-getting-better-healthcare-with-this-cloud-based-solution/#73ad1f1d593b, 2016.
4. The Assoicated Press,”India census says 70 percent live in villages, most are poor,”https://www.seattletimes.com/nation-world/world/india-census-says-70- percent-live-in-villages-most-are-poor/, 2015.
5. Digital Information Security in Healthcare Act(DISHA), https://www.nhp.gov.in/NHPfiles/R_4179_1521627488625_0.pdf, 2017
6. Peter, F.E.,Micelle, J. H., “Health Insurance Portability and Accountability Act(HIPAA),” NCBI, https://www.ncbi.nlm.nih.gov/books/NBK500019/, 2018.
7. Yeh, H.L., Chen, T.H., Liu, P.C., Kim, T.H., and Wei, H.W, “A secured authentication Protocol for wireless sensor networks using elliptic curves cryptography,” sensors,11(5)-4767-4779, 2011.
8. Kumar, P., Lee, S.G., and Lee, H.J., “E-SAP: Efficient-strong authentication protocol for healthcare applications using wireless medical sensor networks,” Sensors, 12(2), 1625-1647, 2012.
9. Shi,w., and Gong, P., “A new user authentication protocol for wireless sensor networks using elliptic curves cryptography,” International journal of distributed sensor networks, Article ID 730831, pp:1-7, doi:10.1155/2013/3730831, 2013.
10. He, D., Kumar, N., Chen, J., Lee, C..-C., Chilamkurti, N., and Yeo,S.-S., “Robust anonymous authentication protocol for health-care application using wireless medical sensor networks,” Multimedia Systems, 21(1), 49-10,2015.
11. Li, X.,Niu, J.,Kumari, S., Liao, J., Liang,W., and Khan, M.K, “A new authentication protocol for healthcare applications using wireless medical sensor networks with user anonymity,” Security and Communication Networks,doi:10.1002/sec.1214, 2015.

References

12. Cremers, C., “The Scyther tool: Verification, Falsification, Analysis of Security Protocols?” In Proceedings of the 20th International Conference on Computer Aided Verification (CAV 2008), Department of Computer Science, ETH Zurich, Switzerland, Princeton, USA, 2008.
13. Dolev, D. and Yao, A.C., “On the Security of Public Key Protocols,” IEEE Transactions on Information Theory, Vol. 29, No. 12, pp.198-208, 1983.
14. Das, M.L., “Two-factor User Authentication in Wireless Sensor Networks,” IEEE Transaction Wireless Communication, 8, pp.1086-1090, 2009.
15. Khan, M.K. and Alghathbar,K., “Cryptanalysis and Security Improvements of Two-Factor User Authentication in Wireless Sensor Networks,” Sensors,10, pp.245-2459, 2010.
16. Vaidya, B.Makrais, D. and Mouftah, H, “Two-Factor Mutual Authentication with Key Agreement in Wireless Sensor Networks,” Available online” https://onlinelibrary.wiley.com/doi/full/10.1002/sec.517, 2012.

Thank You