SmartAuth:

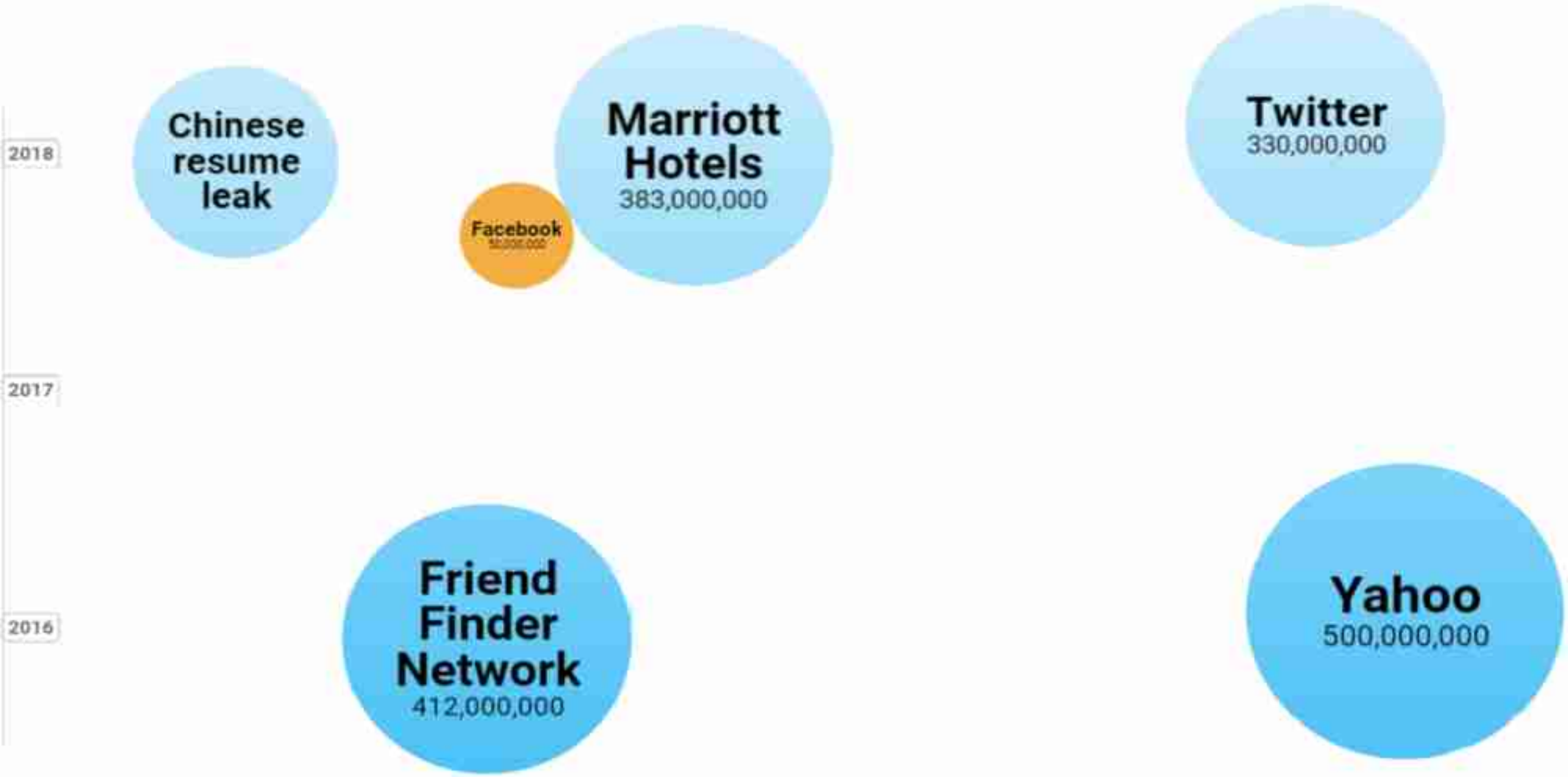
Multi-Factor Authentication using Smart Card and Android on Web

Muhammad Shahbaz

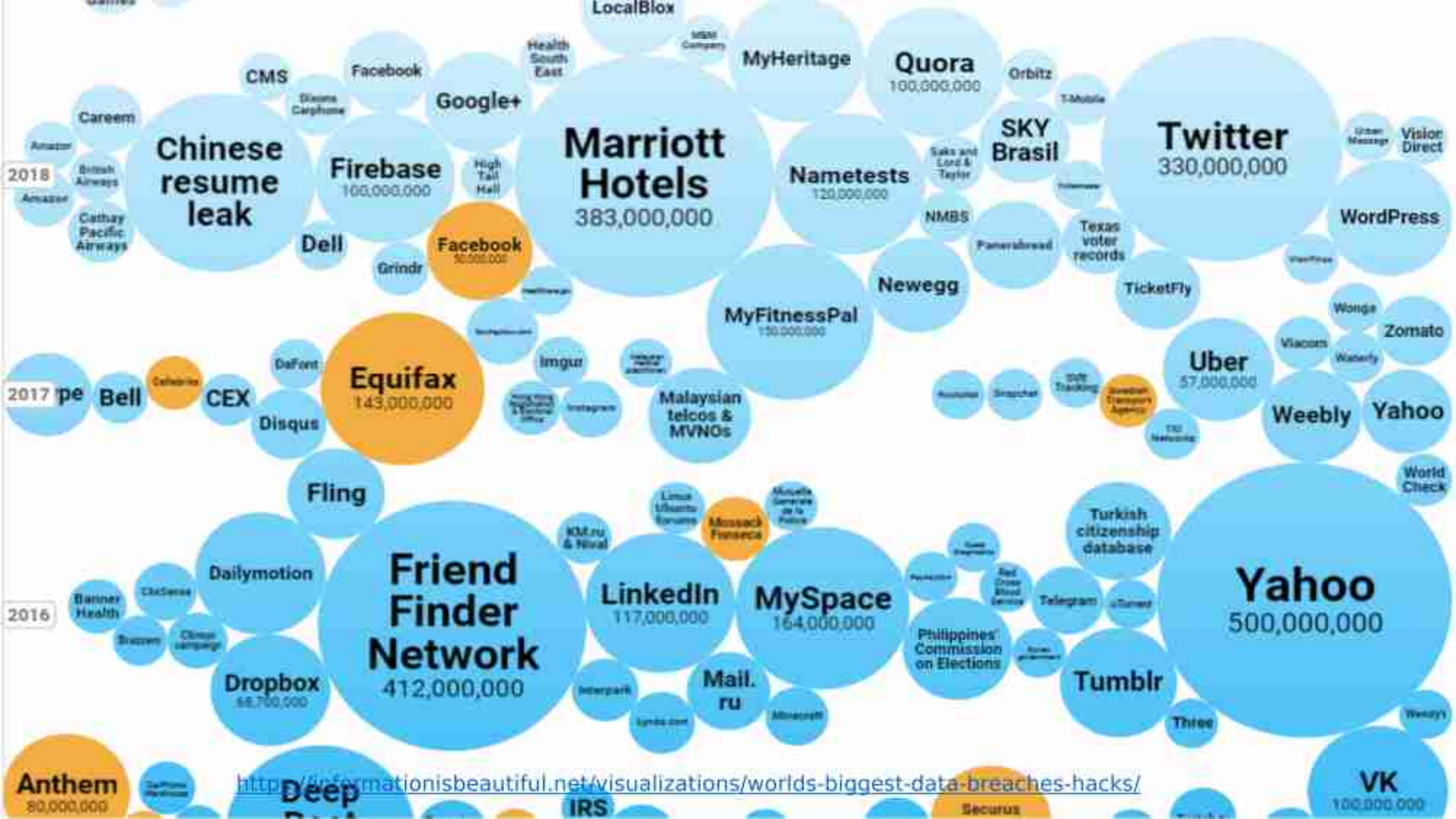
National University of Sciences & Technology
www.nust.edu.pk

NUST
Defining futures

AUTHENTICATION

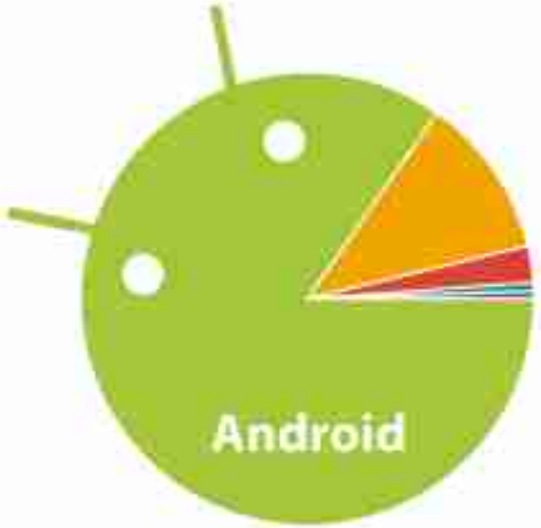


https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/


2018
2017
2016
Chinese resume leak
Marriott Hotels
383,000,000
Firebase
100,000,000
Facebook
50,000,000
Google+
Facebook
CMS
Careem
Dell
Grindr
LocalBlox
MyHeritage
Quora
100,000,000
Orbitz
T-Mobile
SKY Brasil
Twitter
330,000,000
Visior Direct
WordPress
Nametests
120,000,000
NMBS
Panera Bread
Texas voter records
TicketFly
Newegg
MyFitnessPal
150,000,000
Equifax
143,000,000
Imgur
Malaysian telcos & MVNOs
Uber
57,000,000
Wonga
Zomato
Viacom
Weebly
Yahoo
Bell
CEX
Disqus
DaFont
Fling
Friend Finder Network
412,000,000
Dailymotion
Dropbox
68,700,000
LinkedIn
117,000,000
MySpace
164,000,000
Mossack Fonseca
Mail. ru
Philippines' Commission on Elections
Turkish citizenship database
Telegram
Tumblr
Yahoo
500,000,000
World Check
Three
Anthem
80,000,000
Deep
IRS
Securus
VK
100,000,000
https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

MOTIVATION

- **User authentication**
- **Popularity of android smartphones**
- **Smart cards**



OBJECTIVE

An alternative approach for a secure user authentication which provides mutual entity verification using smartphone and smart card for web.


AND
OR
MOBILE
APP
SOMETHING YOU
KNOW
SOMETHING YOU
ARE
SOMETHING YOU
HAVE
VERIFIED

SOMETHING YOU KNOW

- **Top password**
  123456

Username : admin
Password : admin

https://www.linkedin.com/feed/upda[illegible]ity:6497819834137616384/

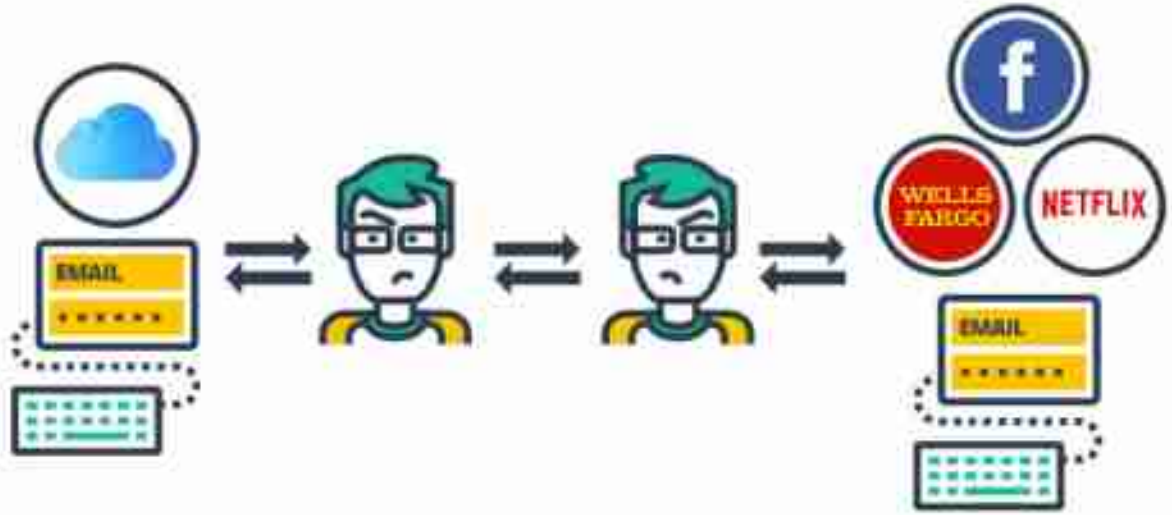
https://www.forbes.com/sites/kateoflahertyuk/2018/12/14/these-are-the-top-20-worst-passwords-of-2018/#629969104541

https://www.linkedin.com/feed/update/urn:li:activity:6402873635

SOMETHING YOU KNOW

Password reuse

- Crucial problem
- AVG 3.9 times same password



2014 - Australian and New Zealand iCloud users were affected, Apple devices got locked for ransom.

https://www.zdnet.com/article/icloud-not-compromised-in-apple-id-attack-apple/
https://security.googleblog.com/2017/11/new-research-understanding-root-cause.html

What Information Was Involved?

Yahoo Breach!

The stolen user account information may have included names, email addresses, telephone numbers, dates of birth, hashed passwords (using MD5) and, in some cases, encrypted or unencrypted security questions and answers. Not all of these

https://pixelprivacy.com/resources/reusing-passwords/

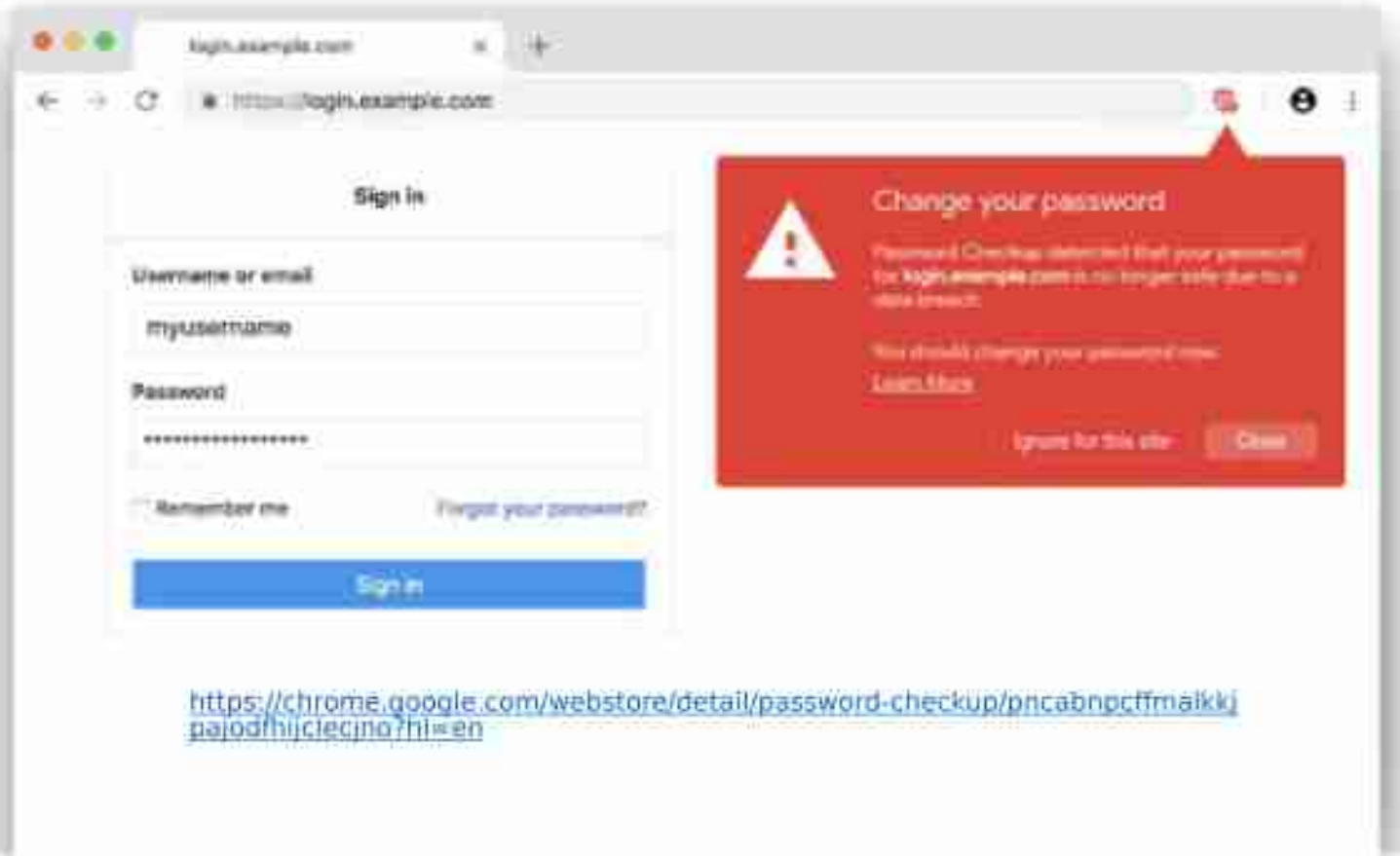
SOMETHING YOU KNOW

https://www.linkedin.com/feed/update/urn:li:activity:6511943014401867776
https://security.googleblog.com/2017/11/new-research-understanding-root-cause.html

SOMETHING YOU KNOW

Password Checkup Chrome Extension by Google

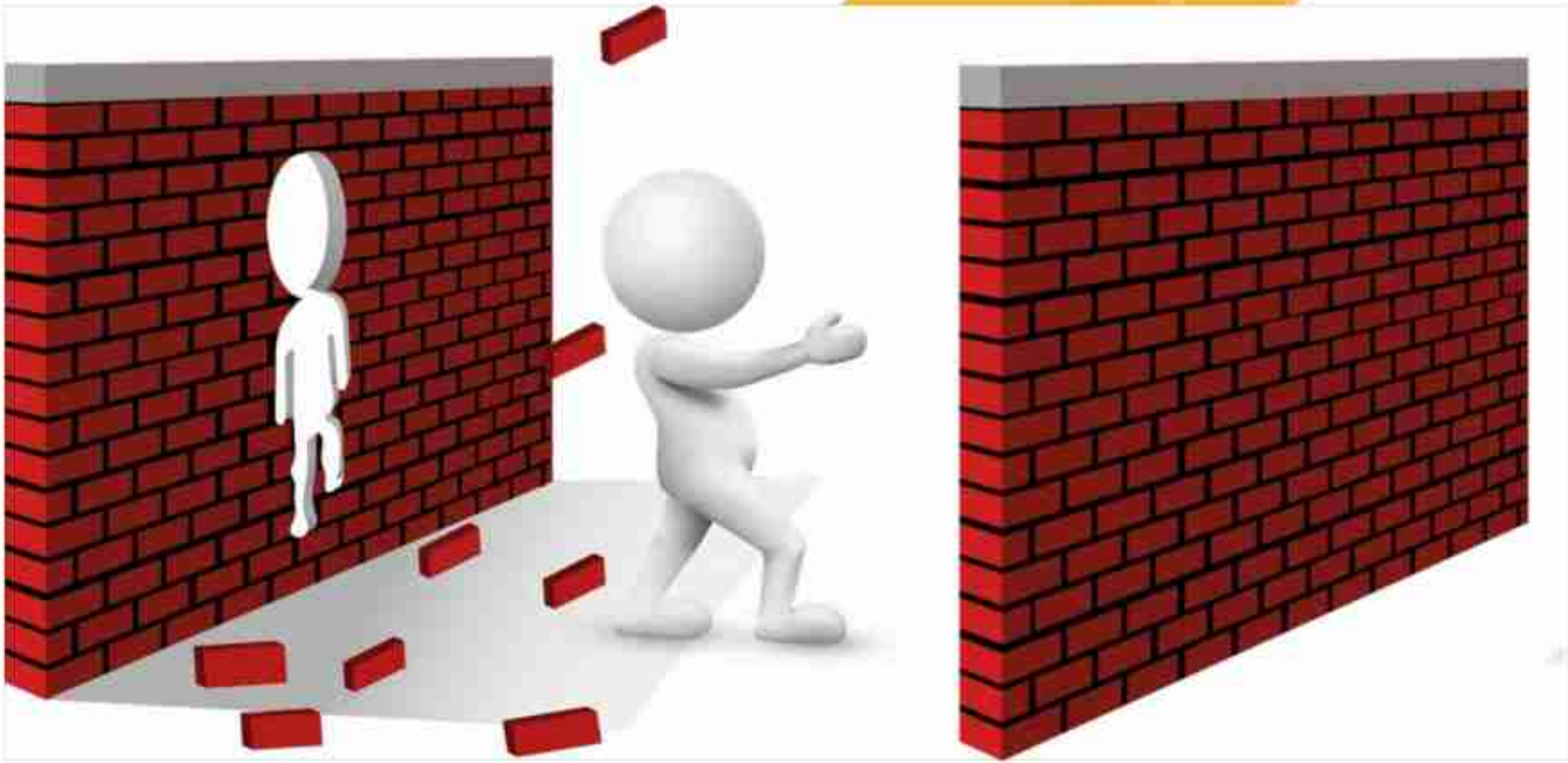
Learn about unsafe accounts wherever you sign in



https://chrome.google.com/webstore/detail/password-checkup/pncabnpcffmaikkjpajodfhijclecjno?hl=en

WEAKEST LINK

DEFENSE IN DEPTH

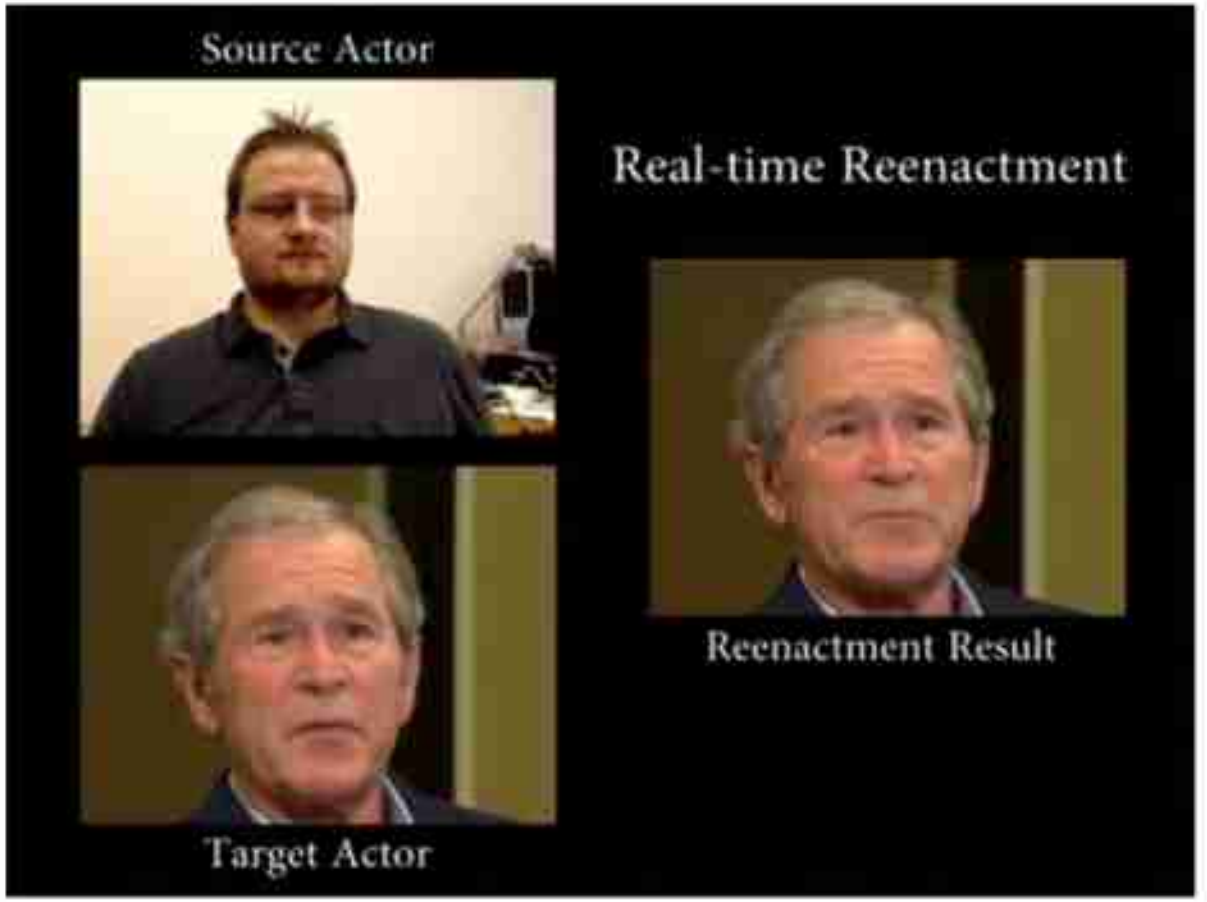


SOMETHING YOU ARE

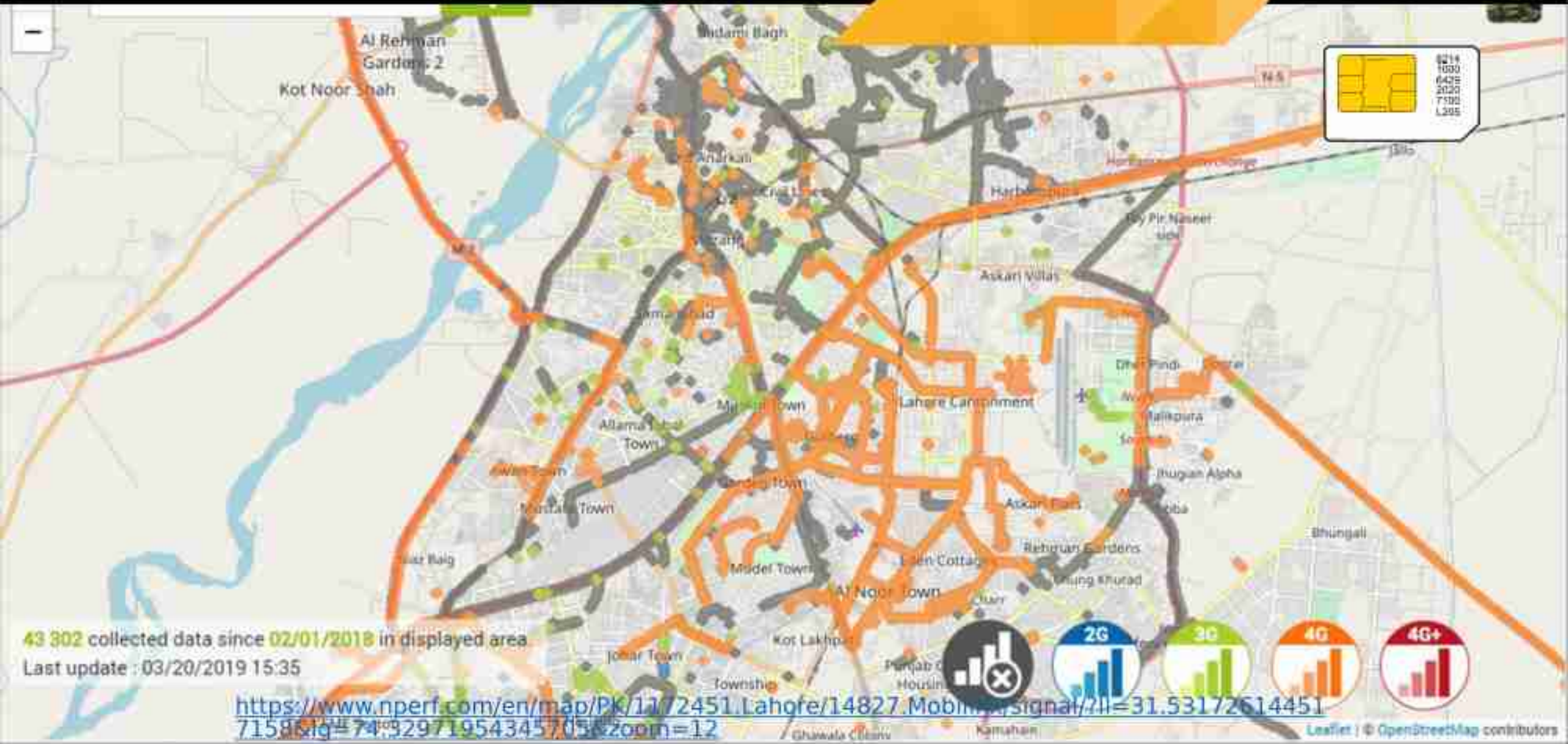
Social Engineering And Emerging Multimedia Technologies - BSides Munich 2018
by Carl Schoeller

https://www.youtube.com/watch?v=rUV5sBChHis&index=14&list=PL8N5HiRDvZ-etExLvF5766VOD0CkZTSZx

SOMETHING YOU ARE



SOMETHING YOU HAVE

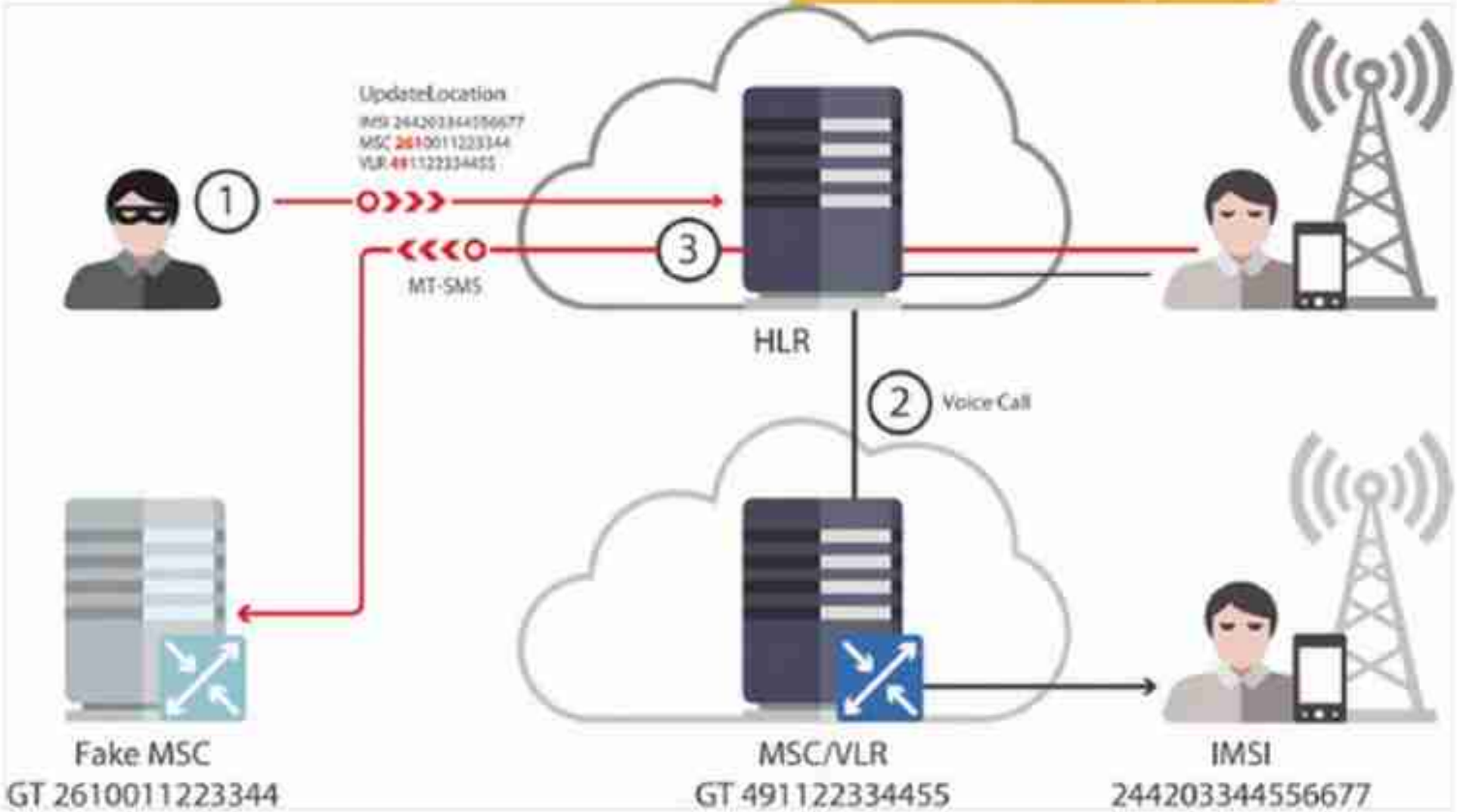


43 302 collected data since 02/01/2018 in displayed area

Last update : 03/20/2019 15:35

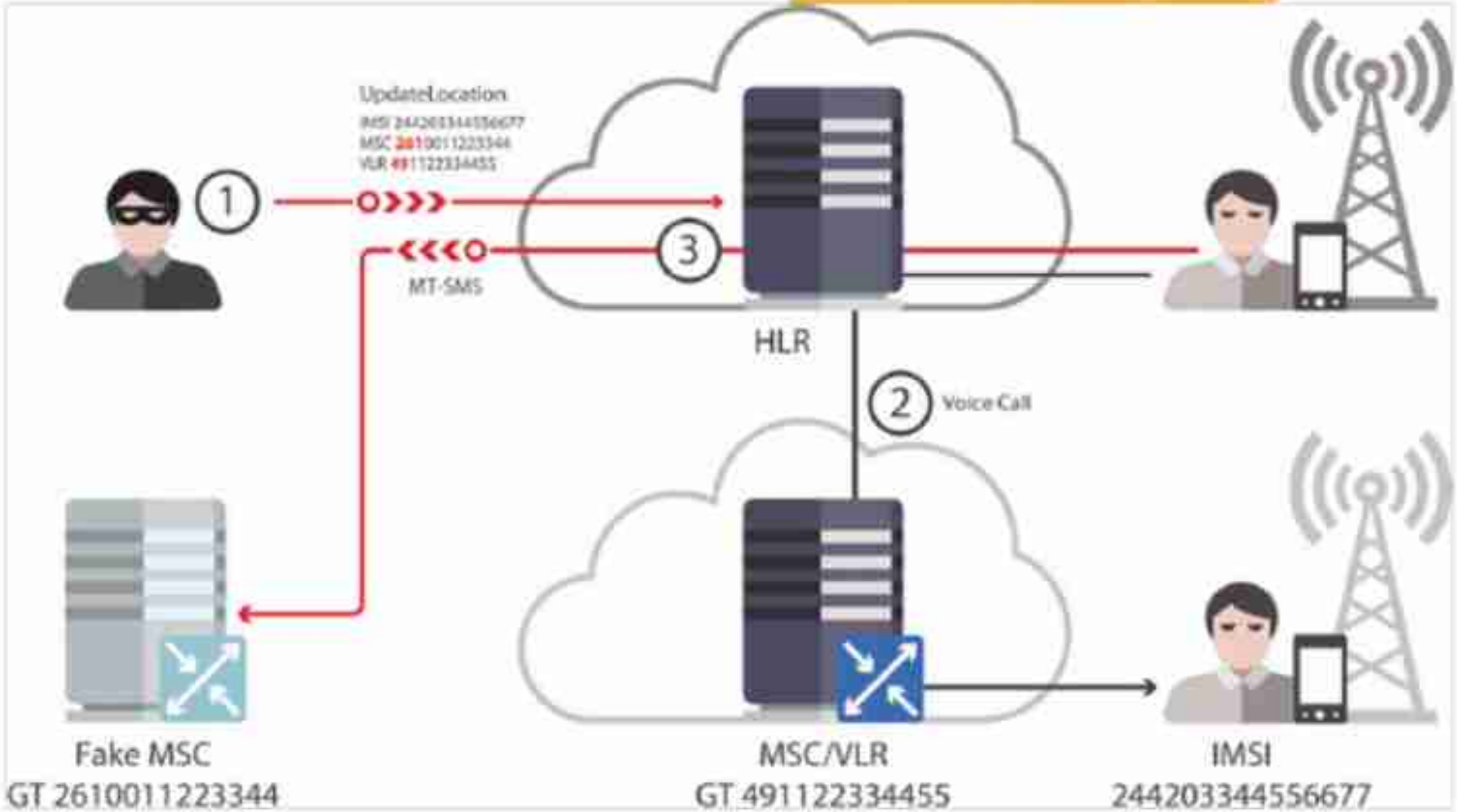
https://www.nperf.com/en/map/PK/1172451.Lahore/14827.Mobile-Signal/?ll=31.531726144517158&lg=74.329719543457058&zoom=12

SS7 VULNERABILITY



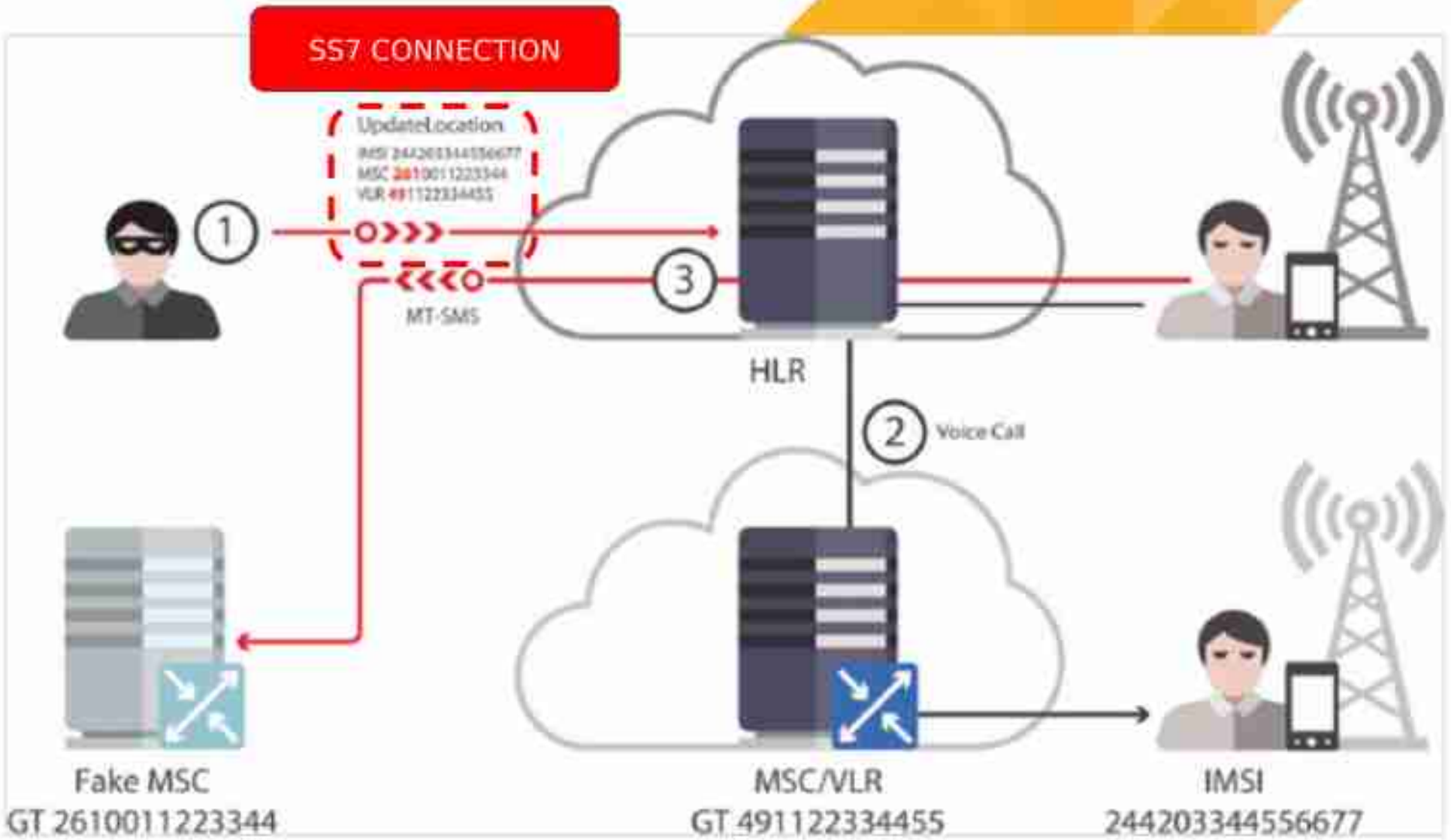
https://www.riverpublishers.com/journal_read_html_article.php?j=JICTS/5/1/2#rfig3

SS7 VULNERABILITY



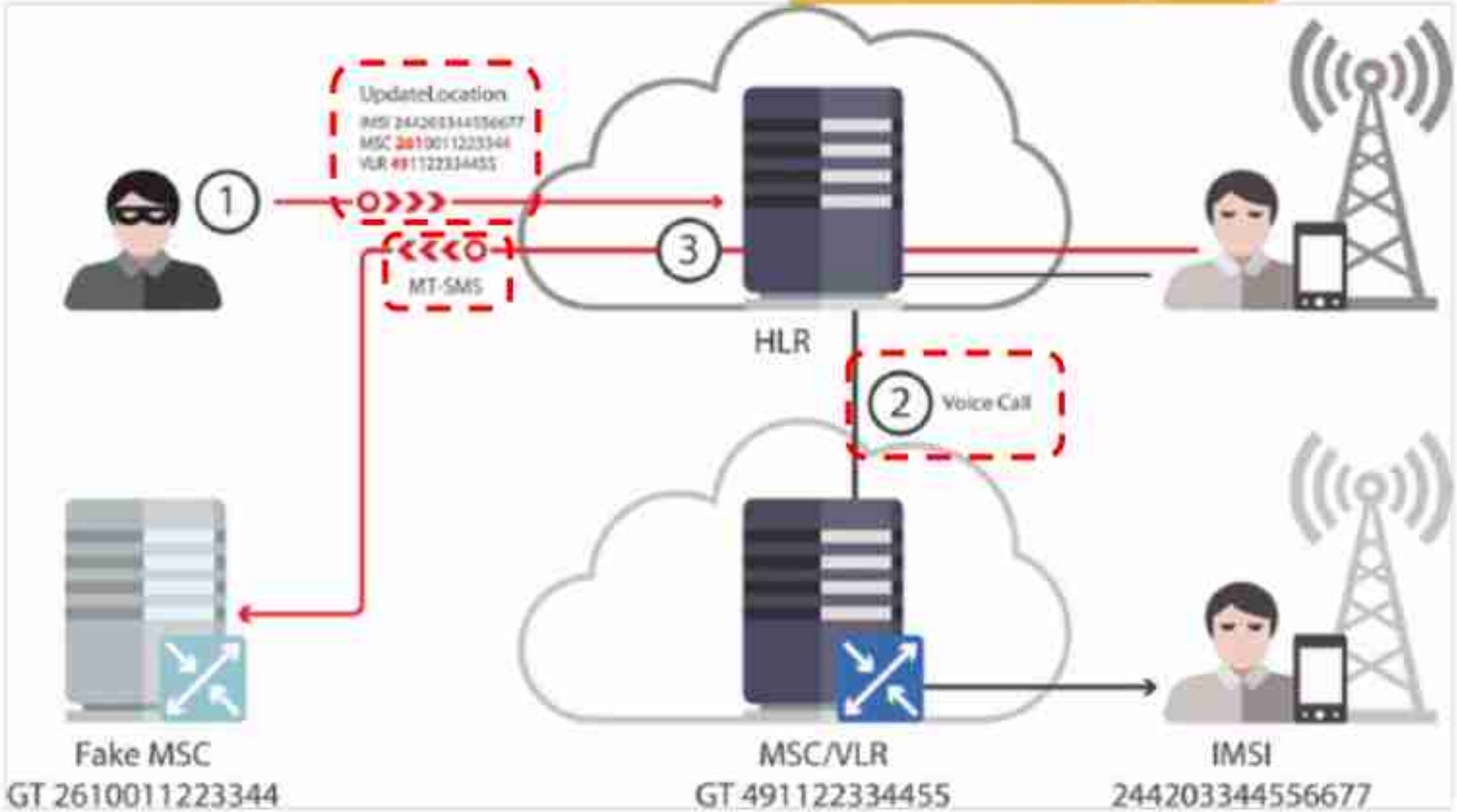
https://www.riverpublishers.com/journal_read_html_article.php?j=JICTS/5/1/2#rfig3

SS7 VULNERABILITY



https://www.riverpublishers.com/journal_read_html_article.php?j=JICTS/5/1/2#rfig3

SS7 VULNERABILITY

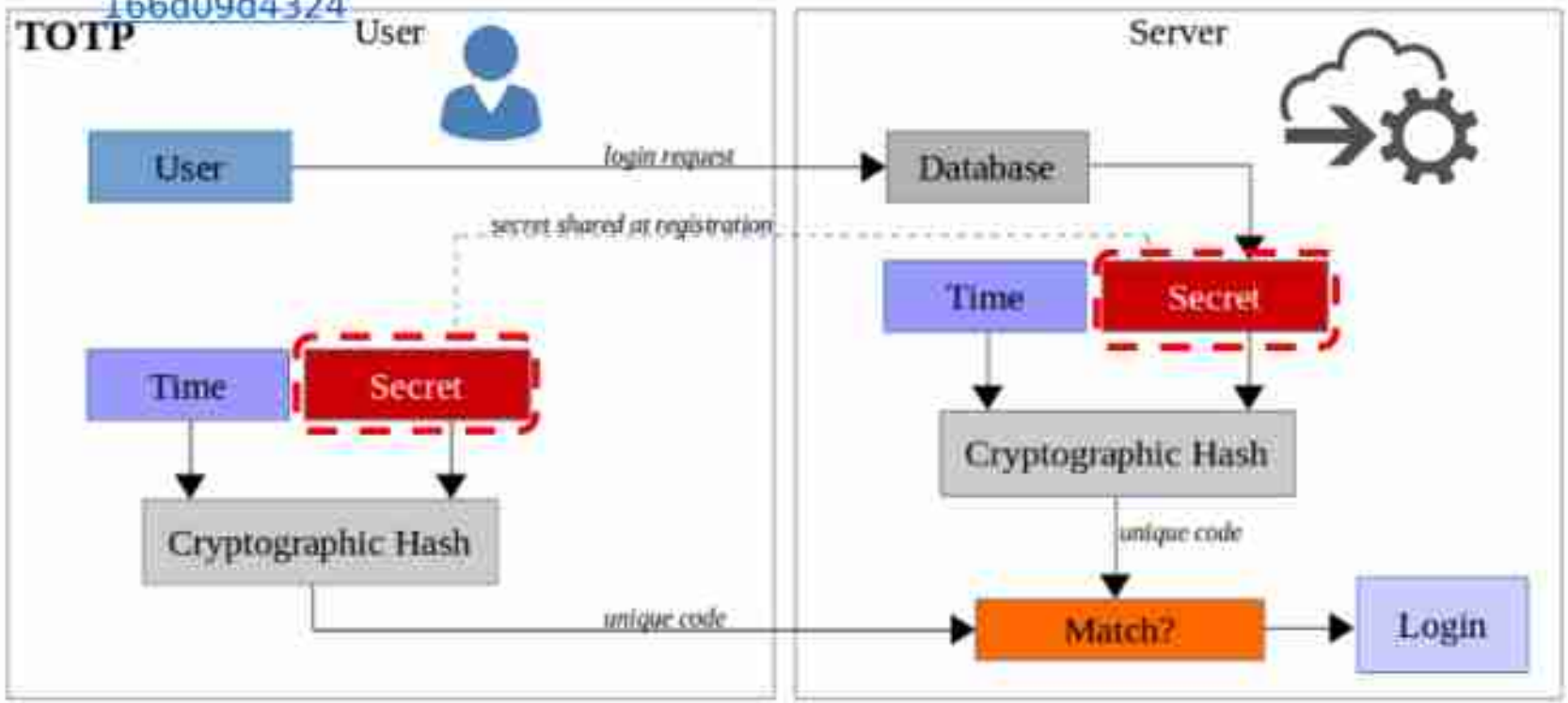


https://www.riverpublishers.com/journal_read_html_article.php?j=JICTS/5/1/2#rfig3

SOMETHING YOU HAVE

Authenticator

https://blog.trezor.io/why-you-should-never-use-google-authenticator-again-e166d09d4324



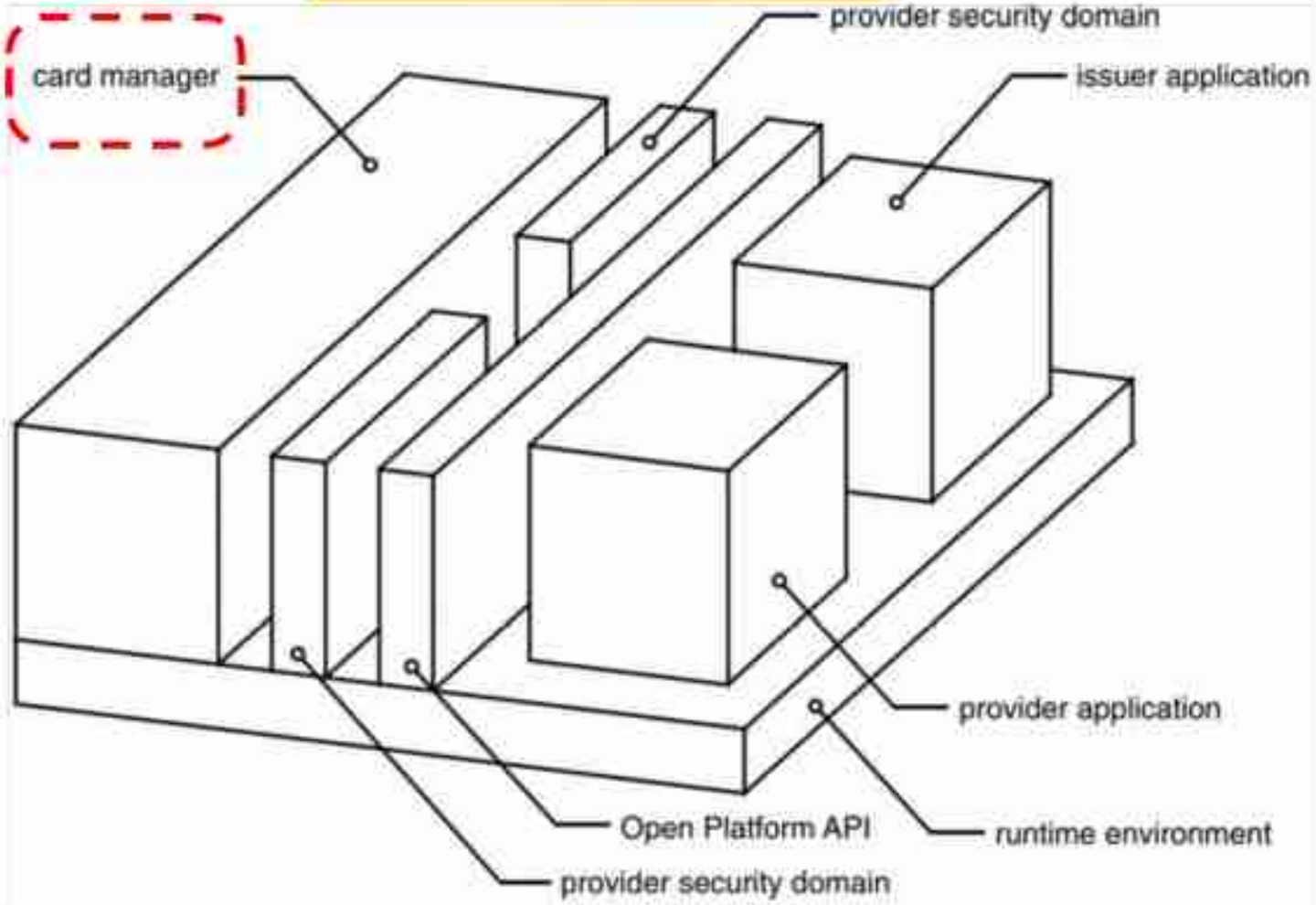
SOMETHING YOU HAVE

SMART CARD

https://www.flickr.com/photos/zapthedingbat/45
0185771/
https://www.flickr.com/photos/zapthedingbat/45
0822010/

SMART CARD

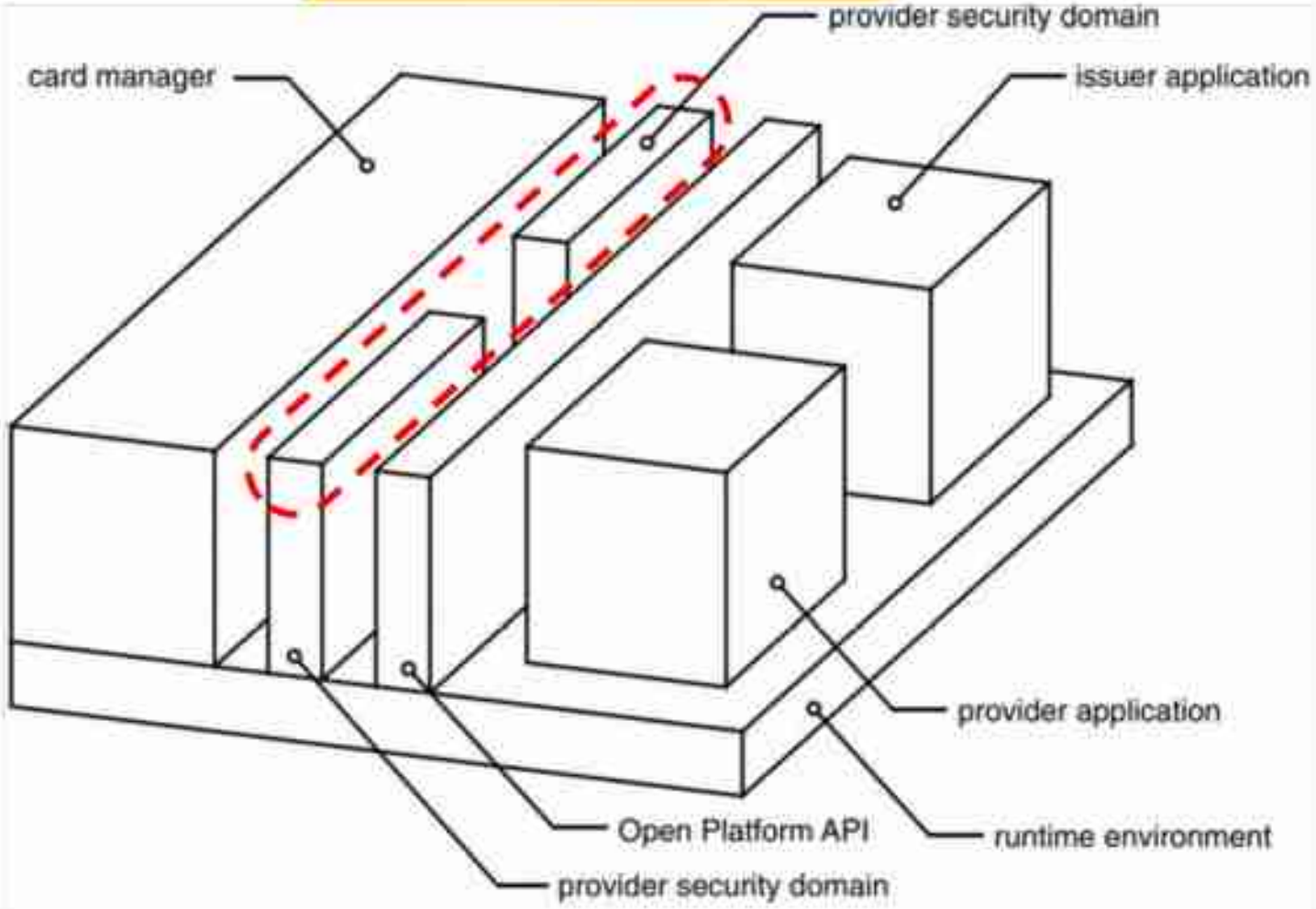
- **OpenPlatform**
- **JCOP**



Rankl, W., & Effing, W. (2004). *Smart card handbook*. John Wiley & Sons.

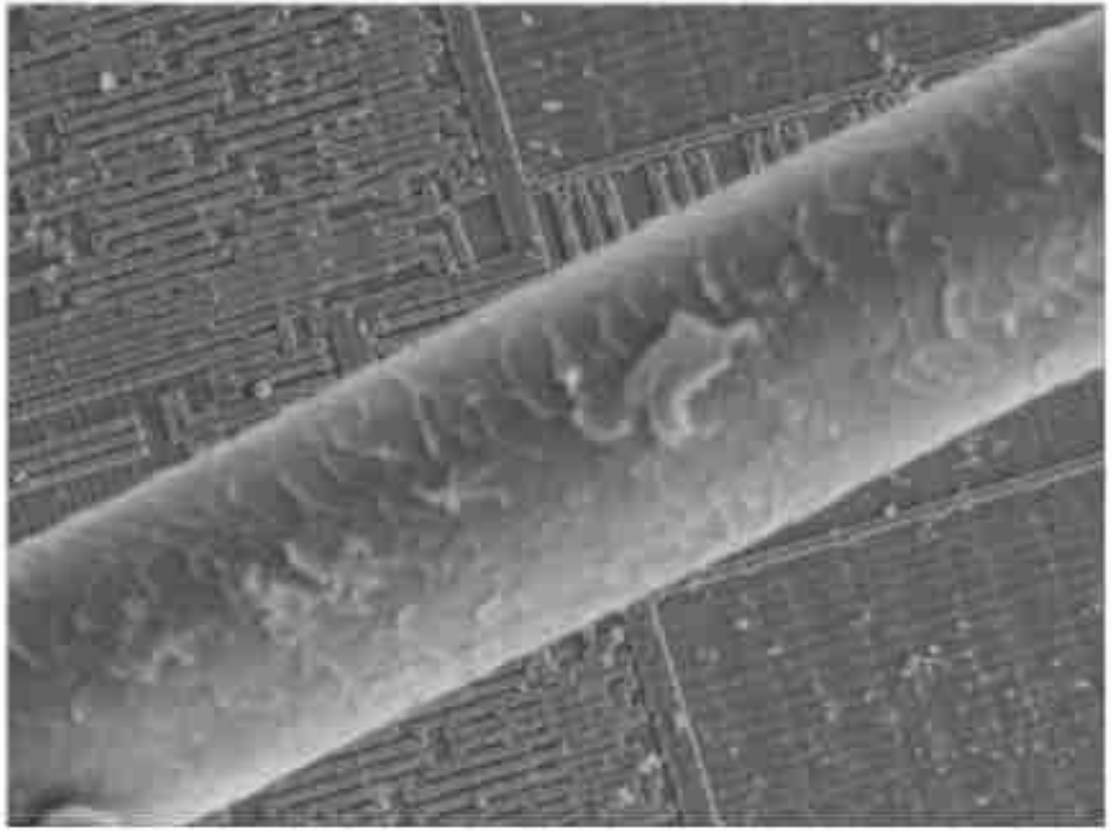
SMART CARD

- **OpenPlatform**
- **JCOP**

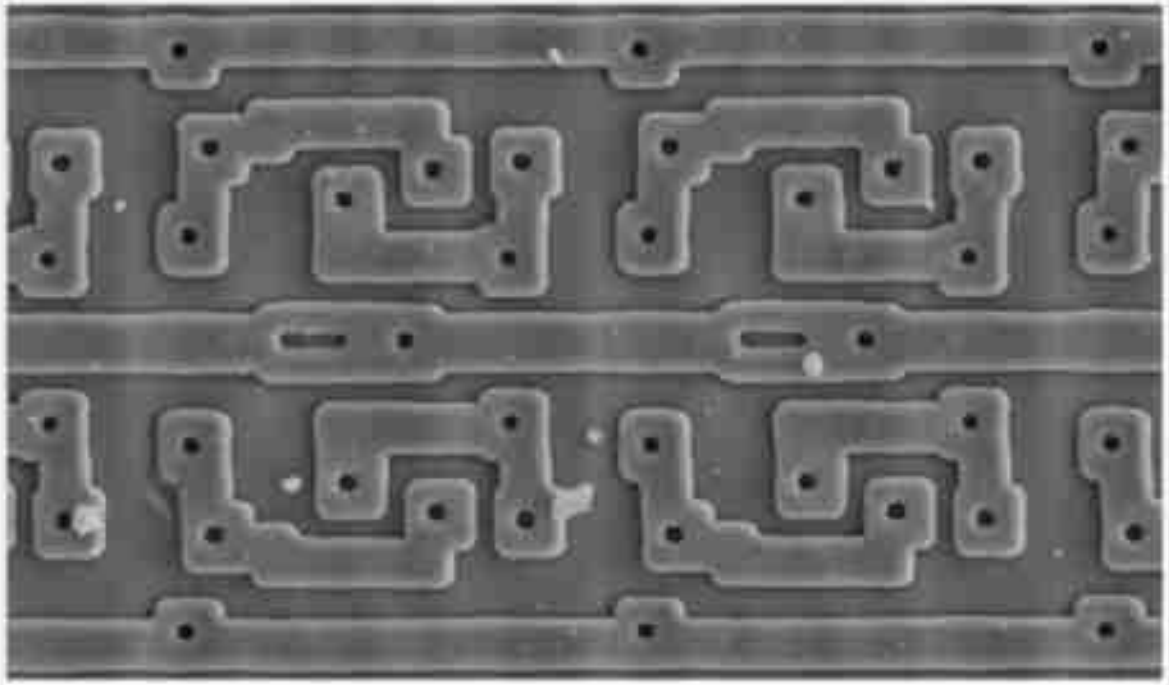


Rankl, W., & Effing, W. (2004). *Smart card handbook*. John Wiley & Sons.

SMART CARD



CHIP
MAGNIFIED 1000×

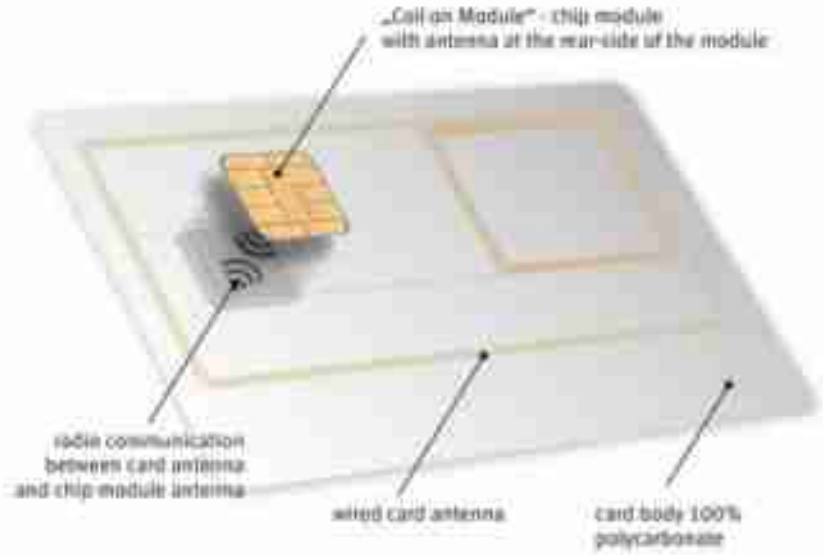


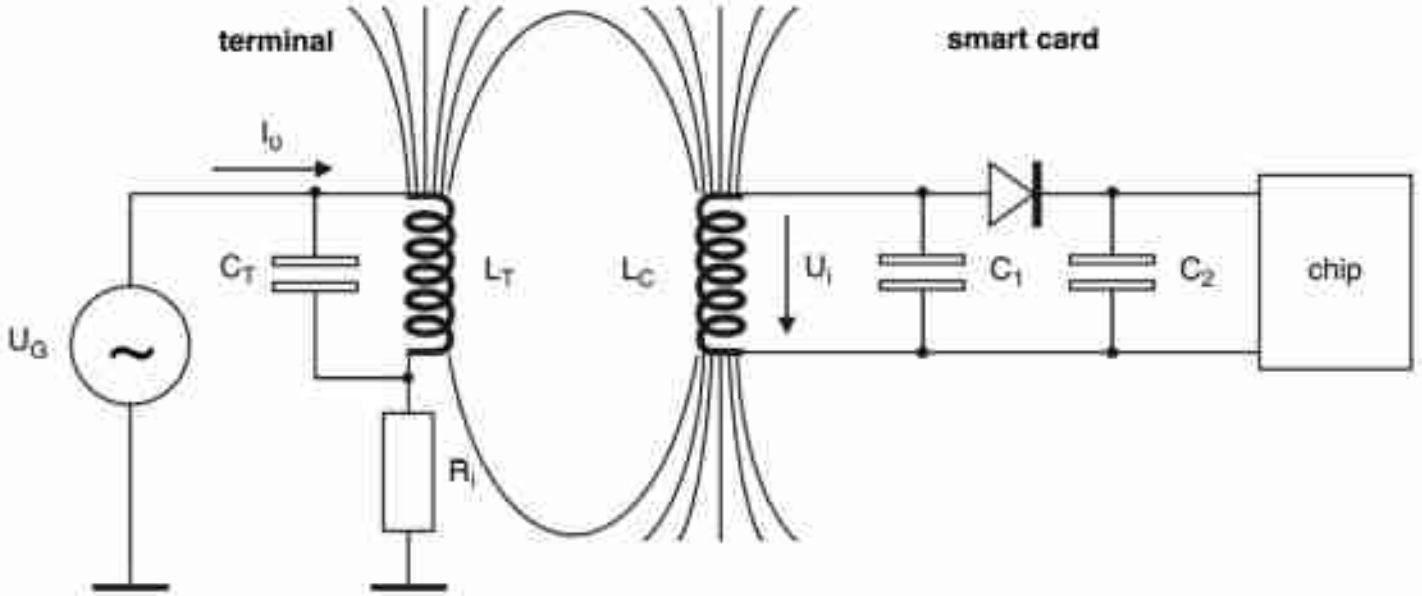
electron beam tester

RAM CELLS
MAGNIFIED 3000×

Rankl, W., & Effing, W. (2004). *Smart card handbook*. John Wiley & Sons.

SMART CARD



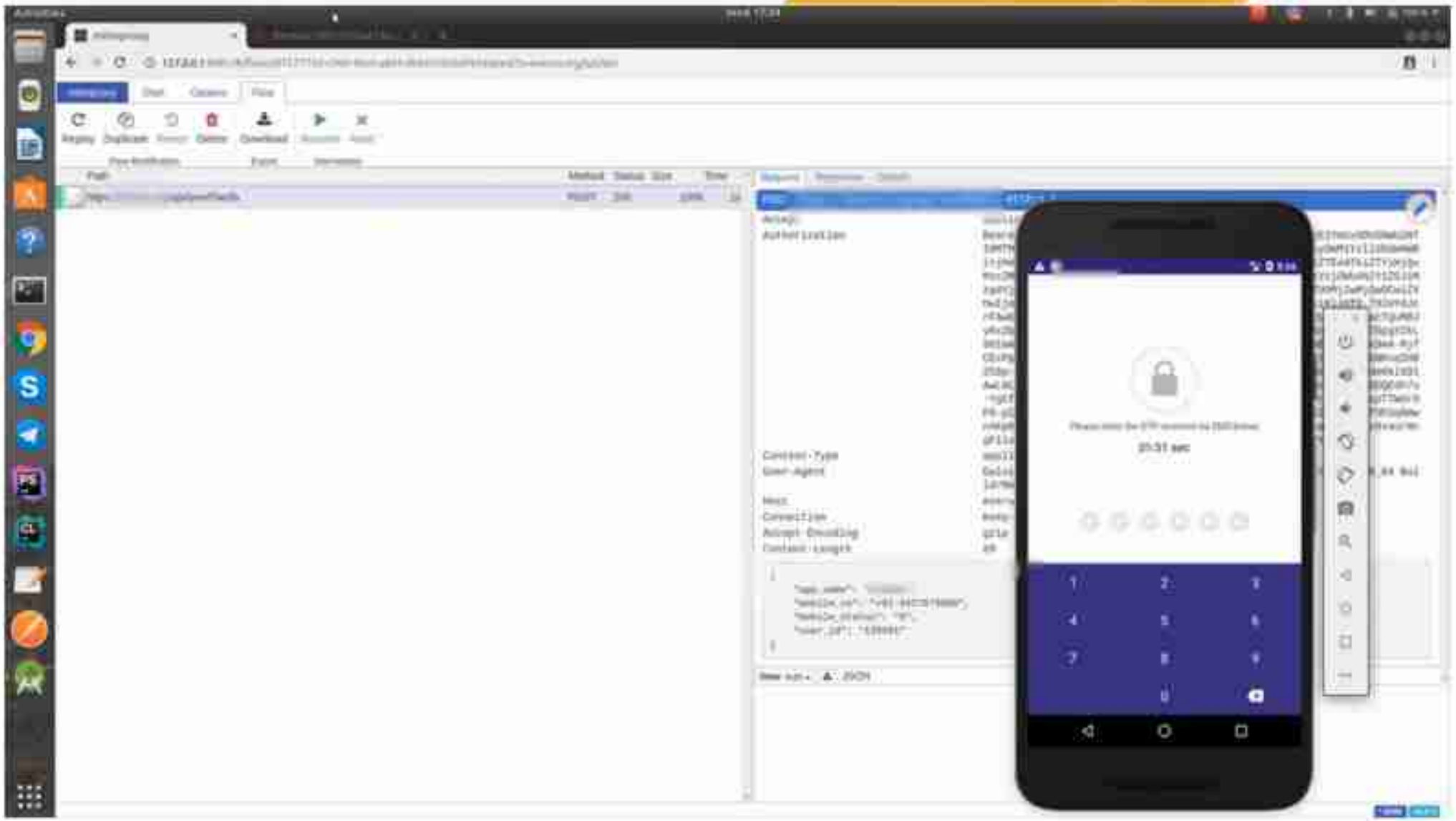


https://www.infineon.com/export/sites/default/media/press/image/press_photo/CoM-for-GovID-en.jpg

Rankl, W., & Effing, W. (2004). *Smart card handbook*. John Wiley & Sons.

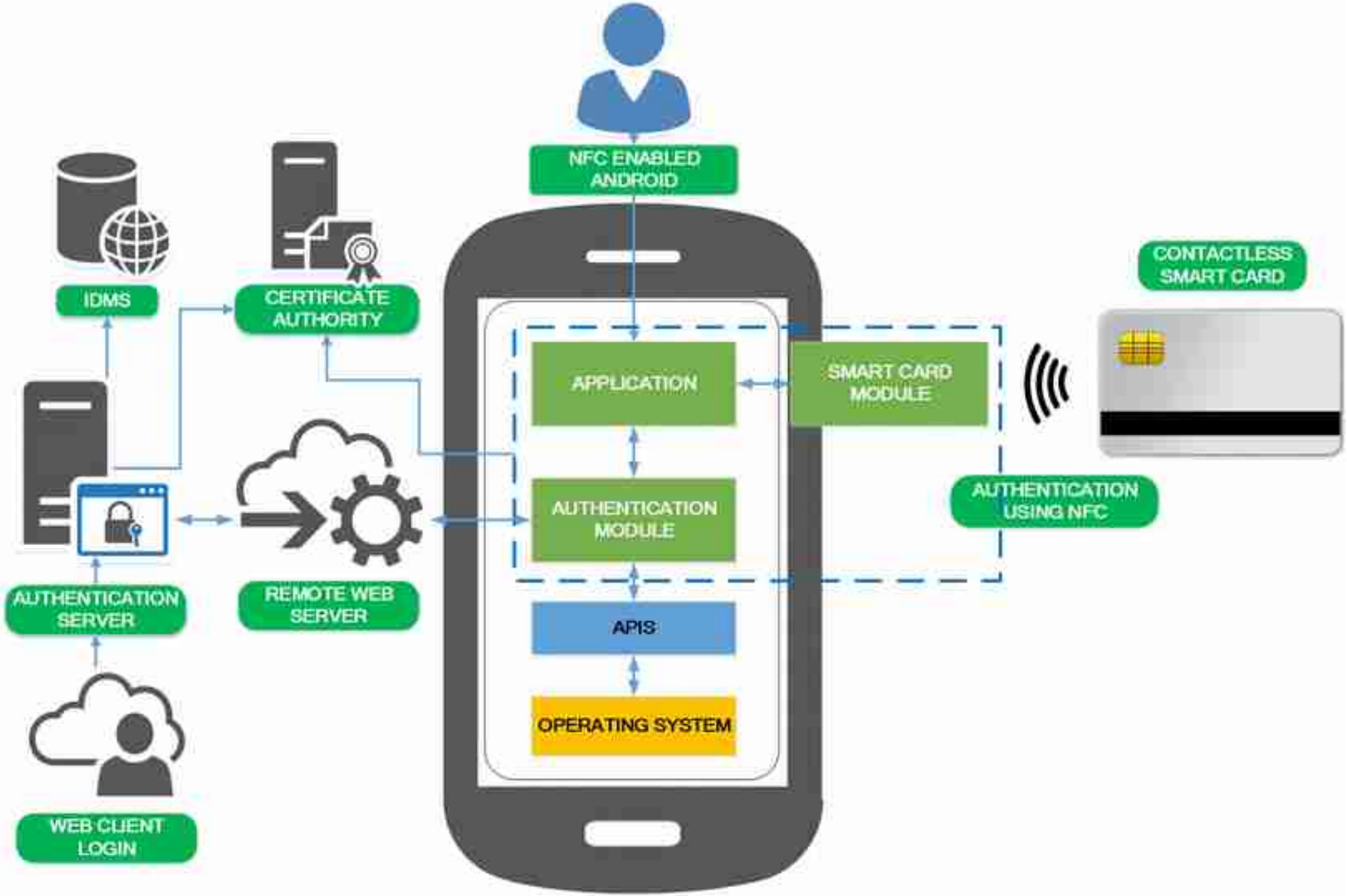
TRUSTED PARTY

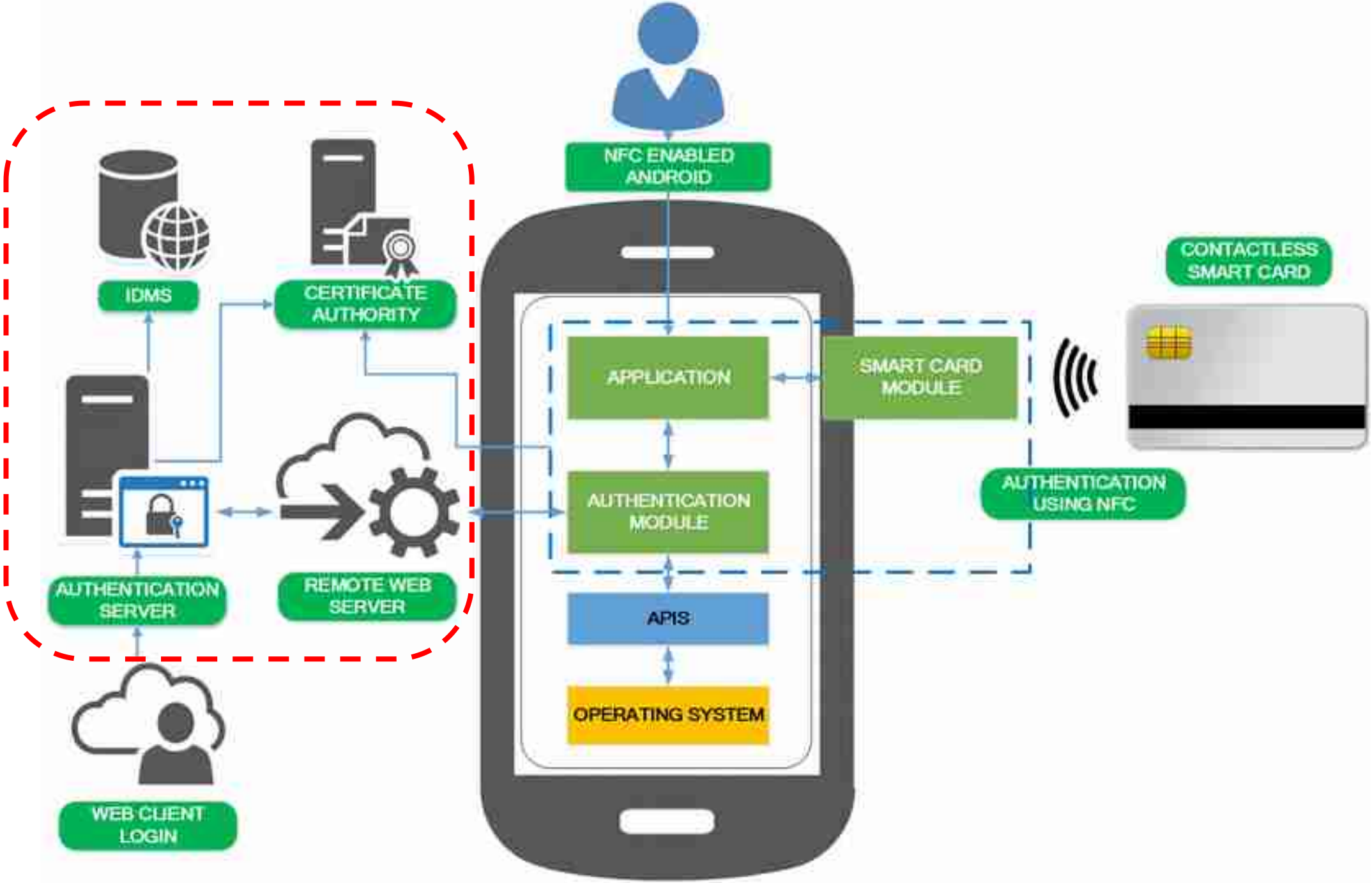
SECURE NOW?

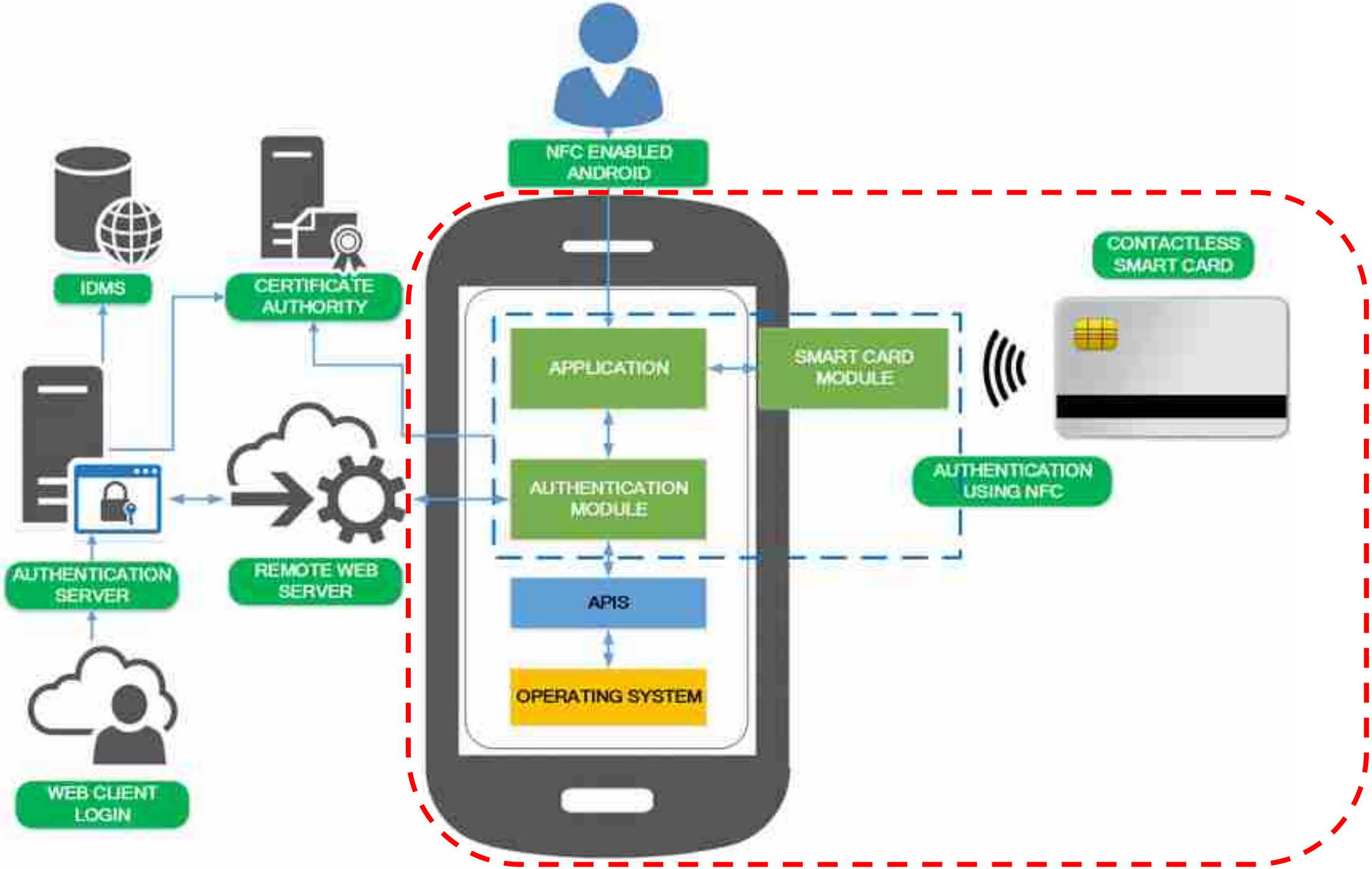


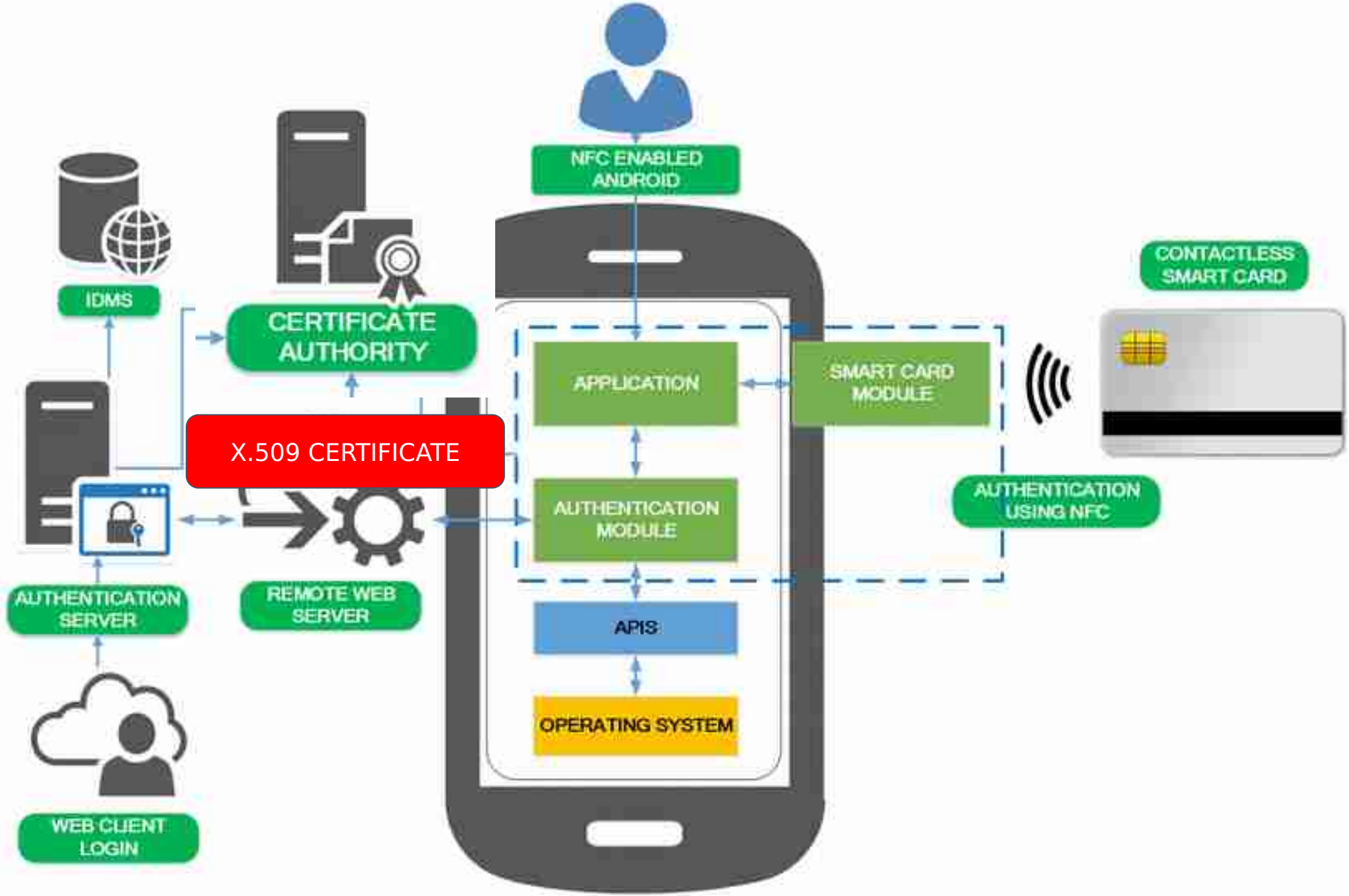
PROPOSED SOLUTION

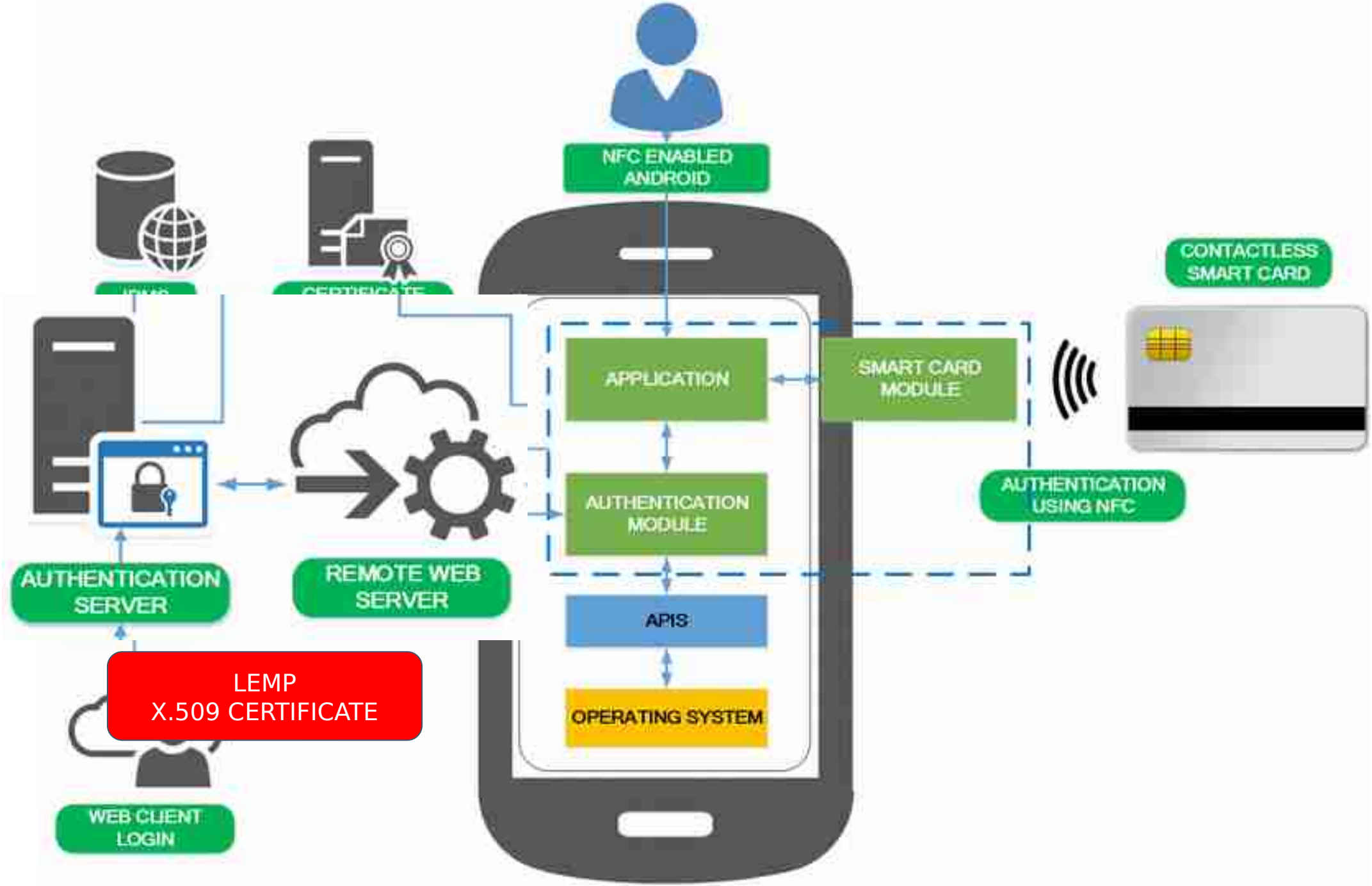
SmartAuth, multi-factor authentication using smart card and android on web with public key cryptography.

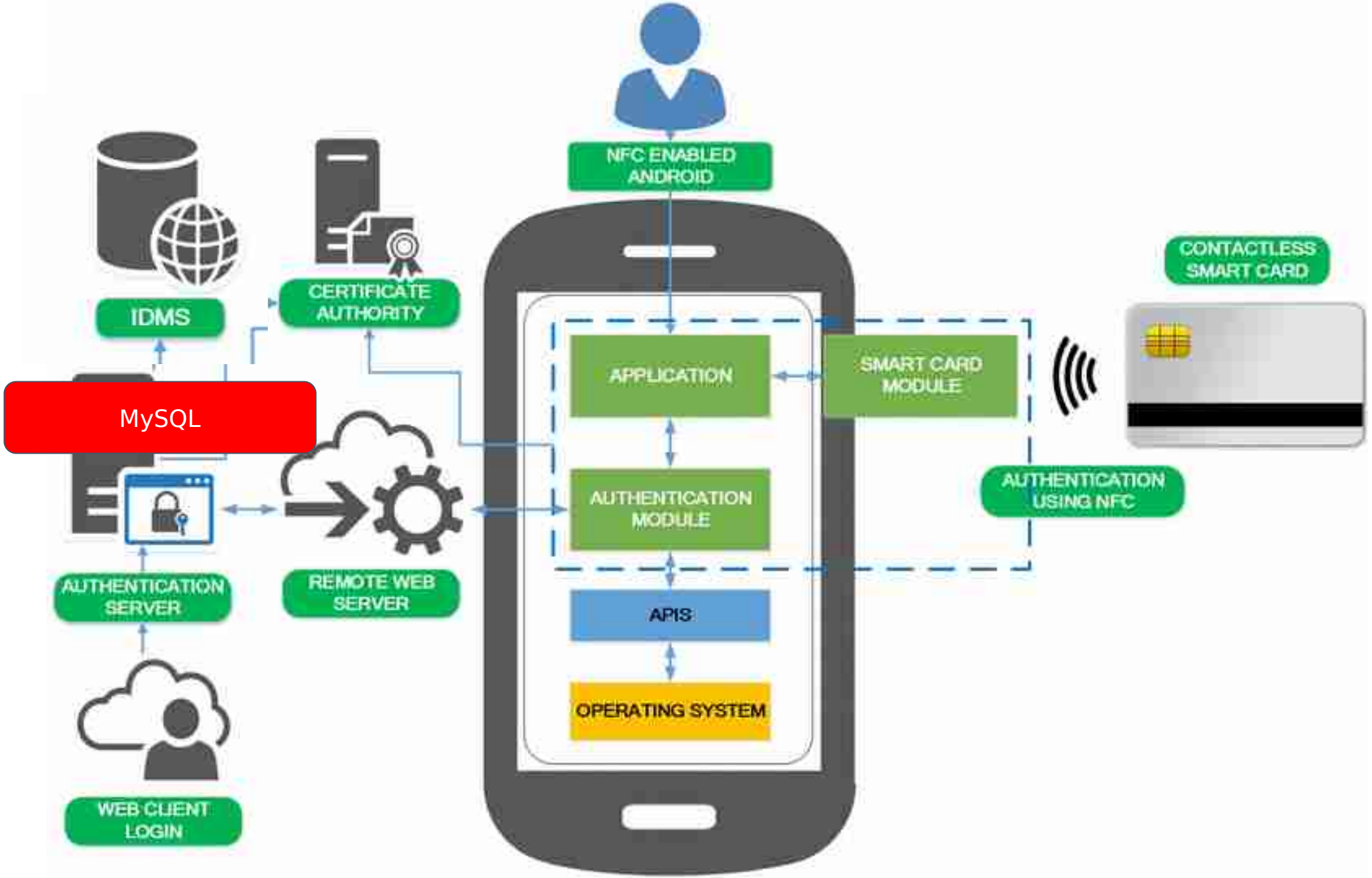

NFC ENABLED ANDROID
IDMS
CERTIFICATE AUTHORITY
CONTACTLESS SMART CARD
APPLICATION
SMART CARD MODULE
AUTHENTICATION MODULE
AUTHENTICATION USING NFC
APIS
OPERATING SYSTEM
AUTHENTICATION SERVER
REMOTE WEB SERVER
WEB CLIENT LOGIN

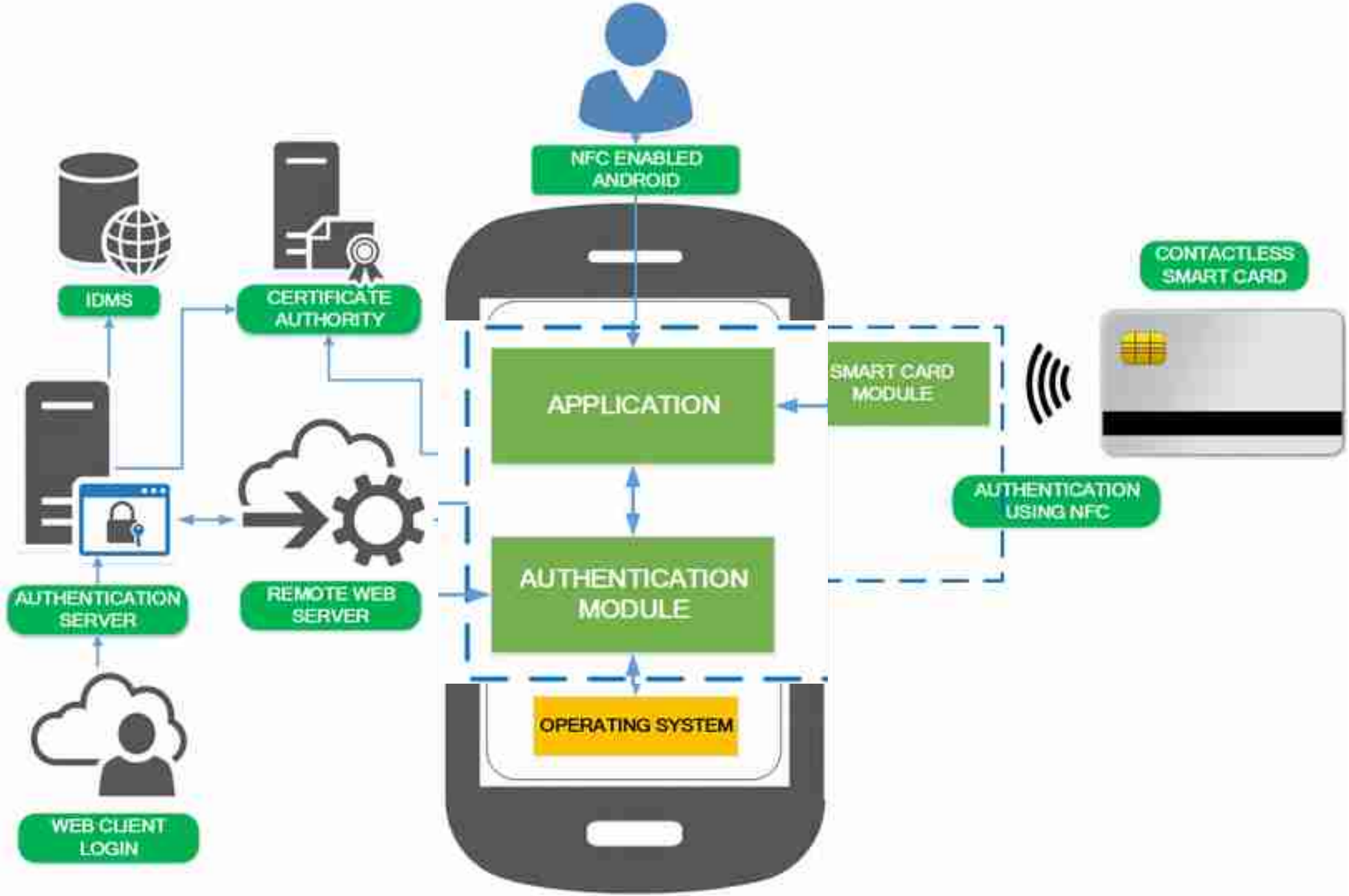

NFC ENABLED ANDROID
IDMS
CERTIFICATE AUTHORITY
APPLICATION
SMART CARD MODULE
CONTACTLESS SMART CARD
AUTHENTICATION MODULE
AUTHENTICATION USING NFC
APIS
OPERATING SYSTEM
AUTHENTICATION SERVER
REMOTE WEB SERVER
WEB CLIENT LOGIN

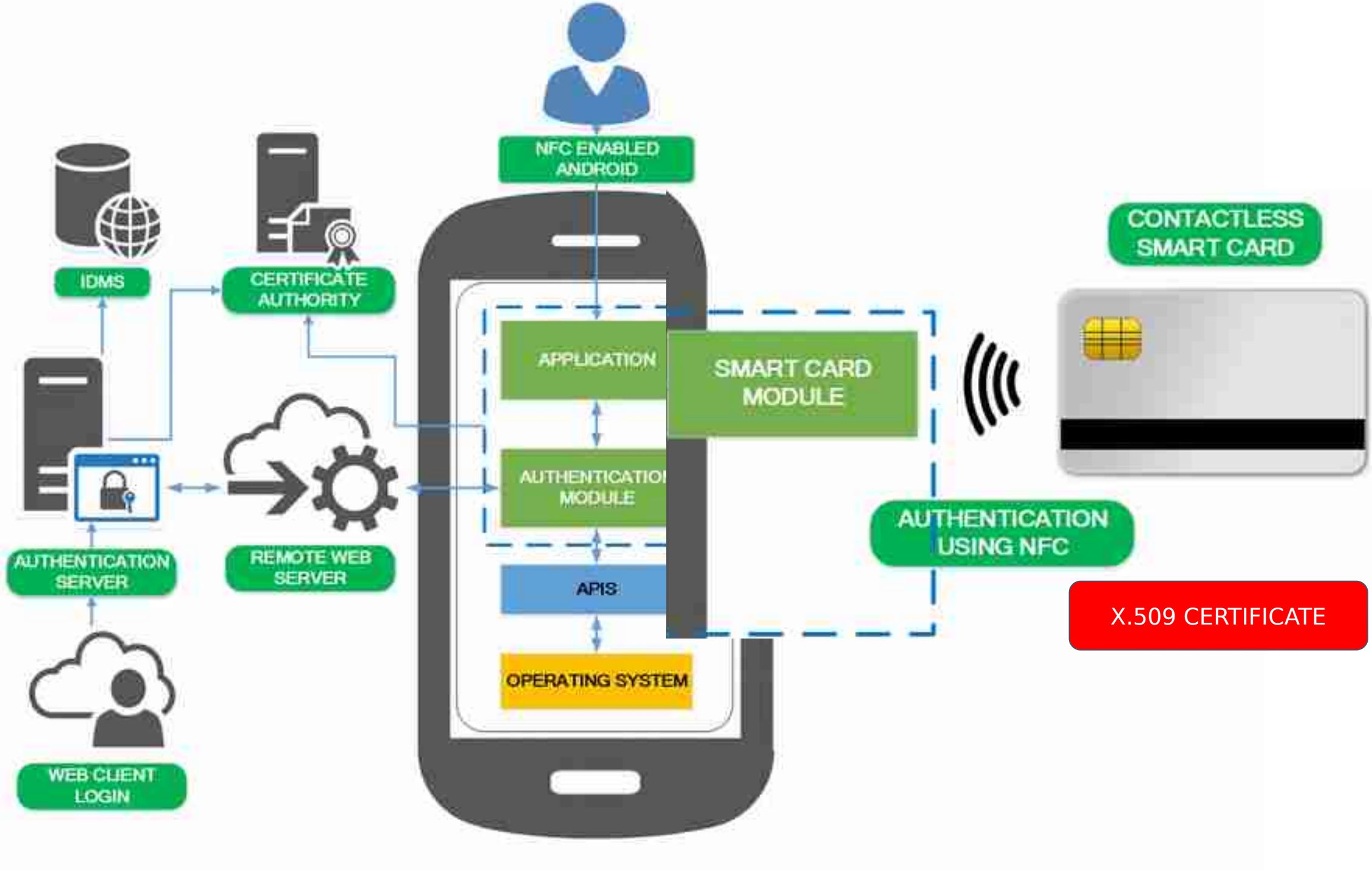

NFC ENABLED ANDROID
IDMS
CERTIFICATE AUTHORITY
CONTACTLESS SMART CARD
APPLICATION
SMART CARD MODULE
AUTHENTICATION MODULE
AUTHENTICATION USING NFC
APIS
OPERATING SYSTEM
AUTHENTICATION SERVER
REMOTE WEB SERVER
WEB CLIENT LOGIN

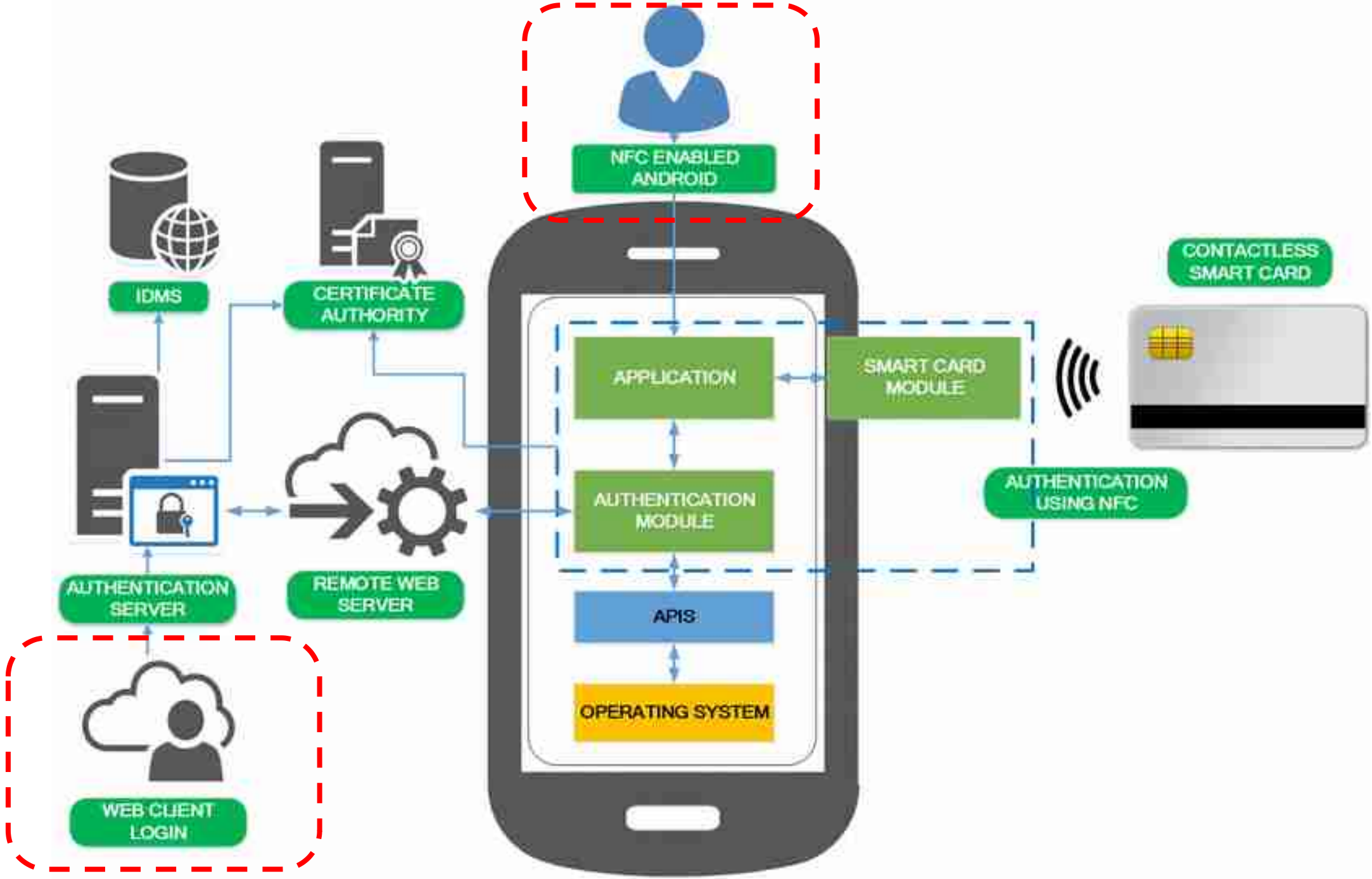

NFC ENABLED ANDROID
IDMS
CERTIFICATE AUTHORITY
CONTACTLESS SMART CARD
APPLICATION
SMART CARD MODULE
X.509 CERTIFICATE
AUTHENTICATION MODULE
AUTHENTICATION USING NFC
AUTHENTICATION SERVER
REMOTE WEB SERVER
APIS
OPERATING SYSTEM
WEB CLIENT LOGIN


NFC ENABLED ANDROID
CONTACTLESS SMART CARD
APPLICATION
SMART CARD MODULE
AUTHENTICATION MODULE
AUTHENTICATION USING NFC
APIS
OPERATING SYSTEM
AUTHENTICATION SERVER
REMOTE WEB SERVER
LEMP
X.509 CERTIFICATE
WEB CLIENT LOGIN


NFC ENABLED ANDROID
IDMS
CERTIFICATE AUTHORITY
MySQL
APPLICATION
SMART CARD MODULE
CONTACTLESS SMART CARD
AUTHENTICATION MODULE
AUTHENTICATION USING NFC
APIS
OPERATING SYSTEM
AUTHENTICATION SERVER
REMOTE WEB SERVER
WEB CLIENT LOGIN

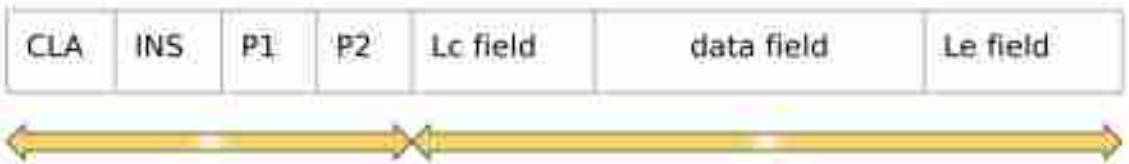

NFC ENABLED ANDROID
IDMS
CERTIFICATE AUTHORITY
CONTACTLESS SMART CARD
APPLICATION
SMART CARD MODULE
AUTHENTICATION USING NFC
AUTHENTICATION SERVER
REMOTE WEB SERVER
AUTHENTICATION MODULE
OPERATING SYSTEM
WEB CLIENT LOGIN


NFC ENABLED ANDROID
IDMS
CERTIFICATE AUTHORITY
APPLICATION
SMART CARD MODULE
AUTHENTICATION MODULE
APIS
OPERATING SYSTEM
CONTACTLESS SMART CARD
AUTHENTICATION USING NFC
AUTHENTICATION SERVER
REMOTE WEB SERVER
WEB CLIENT LOGIN
X.509 CERTIFICATE

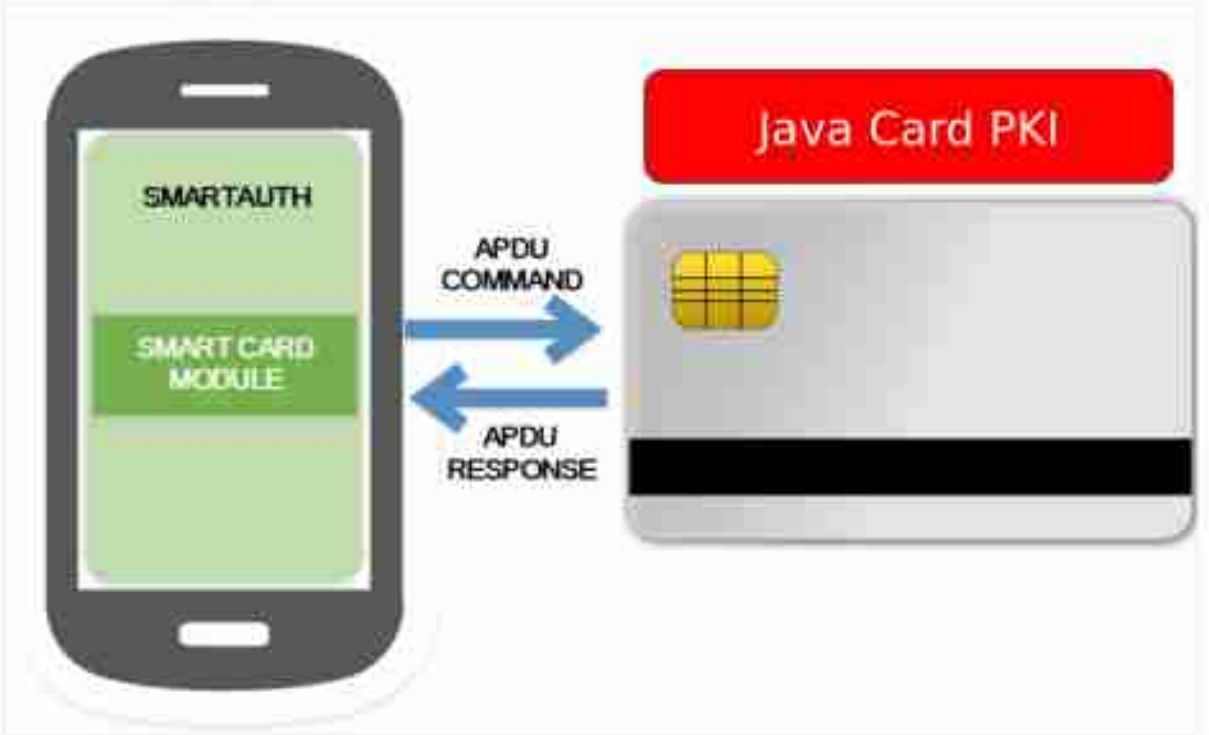

NFC ENABLED ANDROID
IDMS
CERTIFICATE AUTHORITY
CONTACTLESS SMART CARD
APPLICATION
SMART CARD MODULE
AUTHENTICATION MODULE
AUTHENTICATION USING NFC
APIS
OPERATING SYSTEM
AUTHENTICATION SERVER
REMOTE WEB SERVER
WEB CLIENT LOGIN

SMARTCARD MODULE

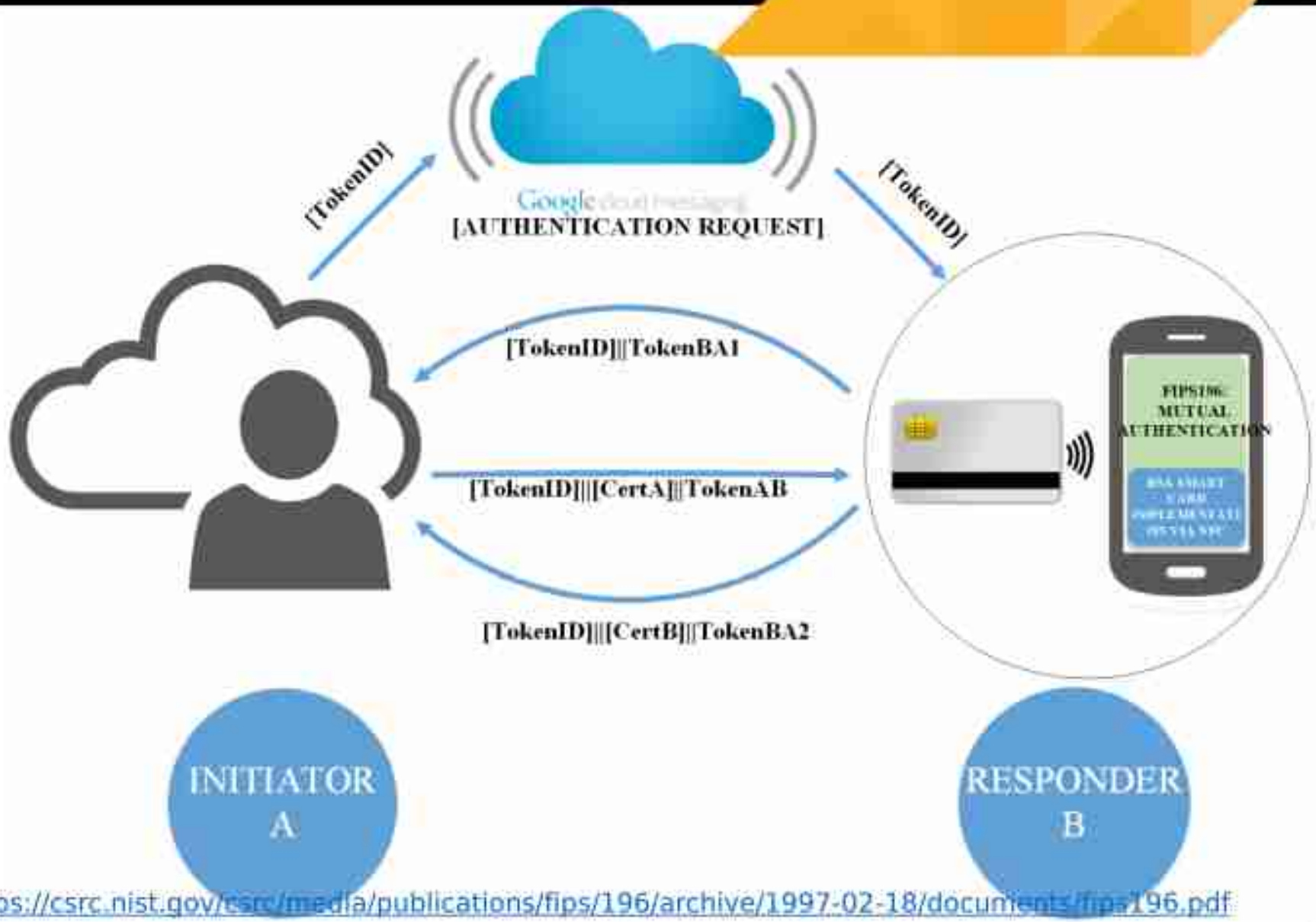
NFC Technology	Protocol Description
NfcA	NFC-A (ISO 14443-3A)
NfcB	NFC-B (ISO 14443-3B)
NfcF	NFC-F (JIS 6319-4)
NfcV	NFC-V (ISO 15693)
IsoDep	ISO-DEP (ISO 14443-4)
Ndef	NFC Forum data format
NdefFormatable	NDEF formattable



APDU - Application protocol data unit
ISO/IEC 7816-4

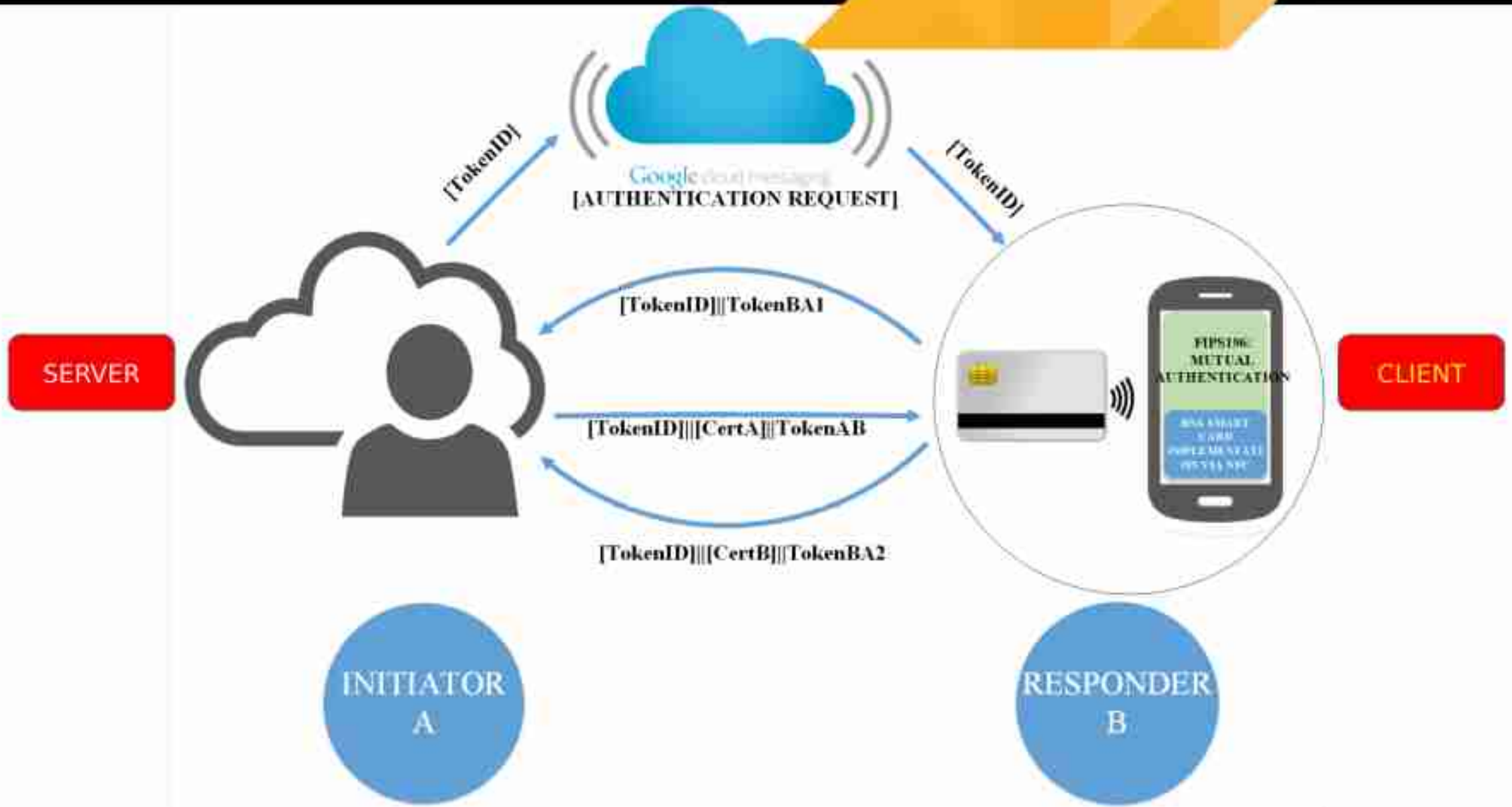


FIPS196 ON WEB

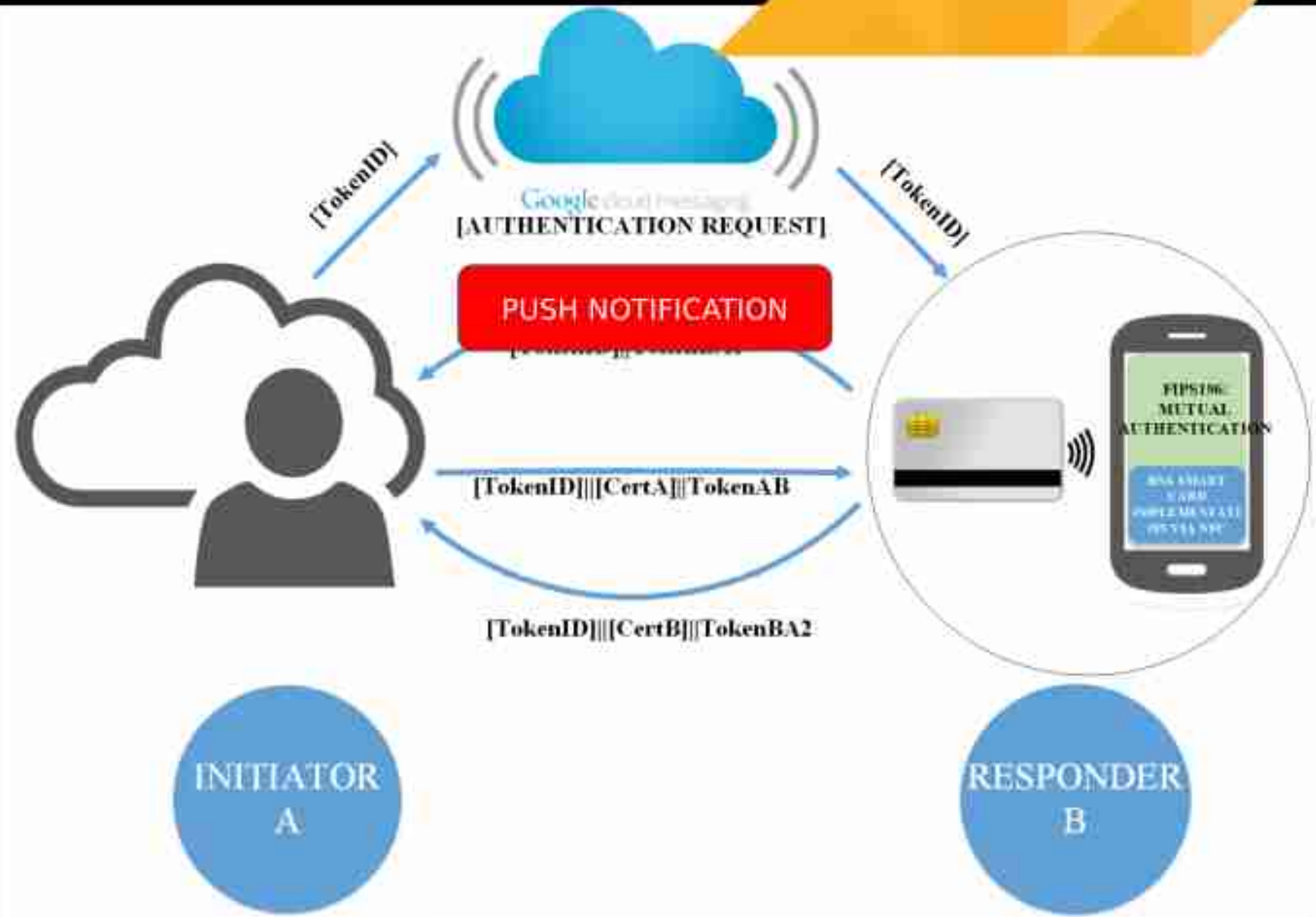


https://csrc.nist.gov/csrc/media/publications/fips/196/archive/1997-02-18/documents/fips196.pdf

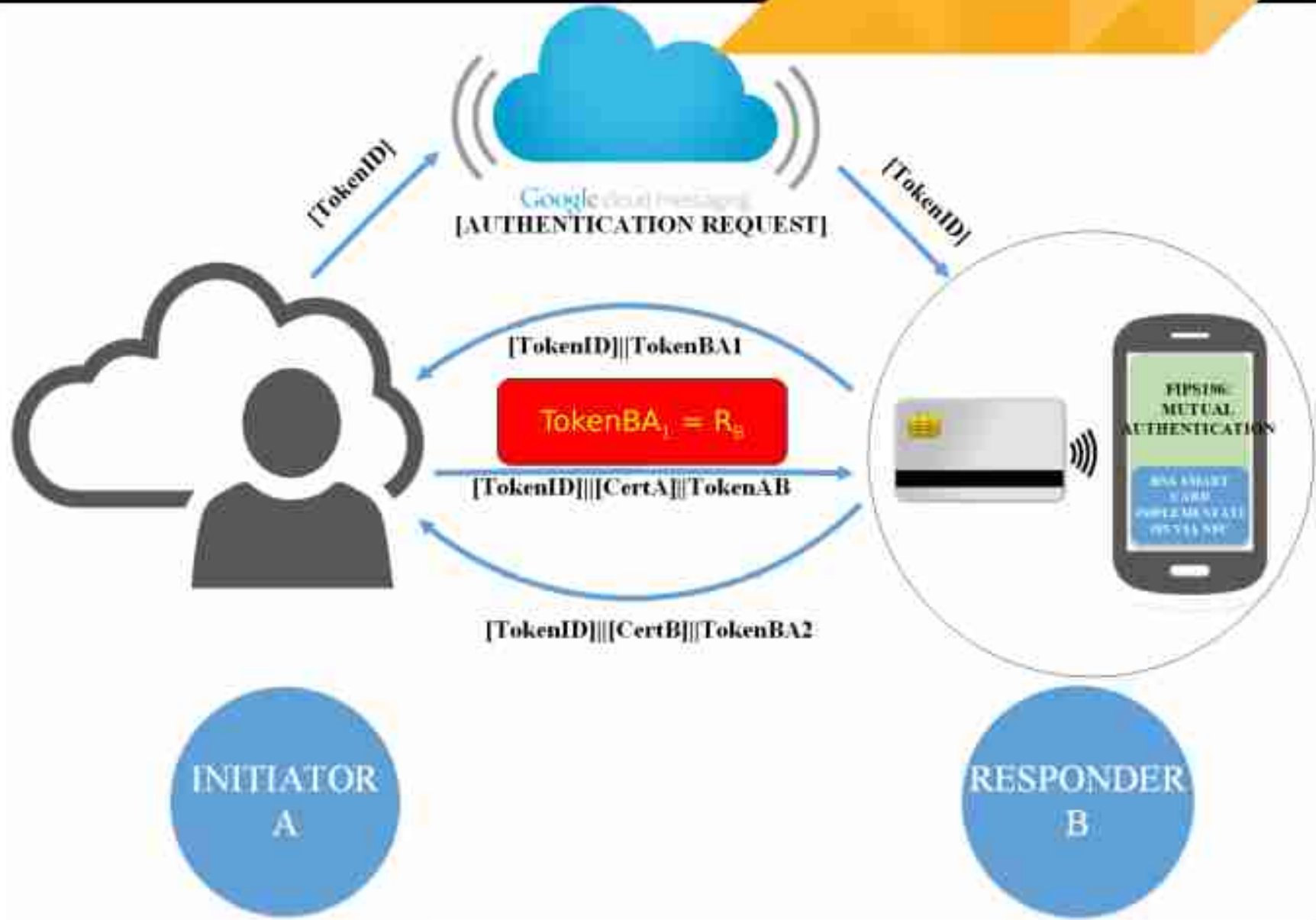
FIPS196 ON WEB



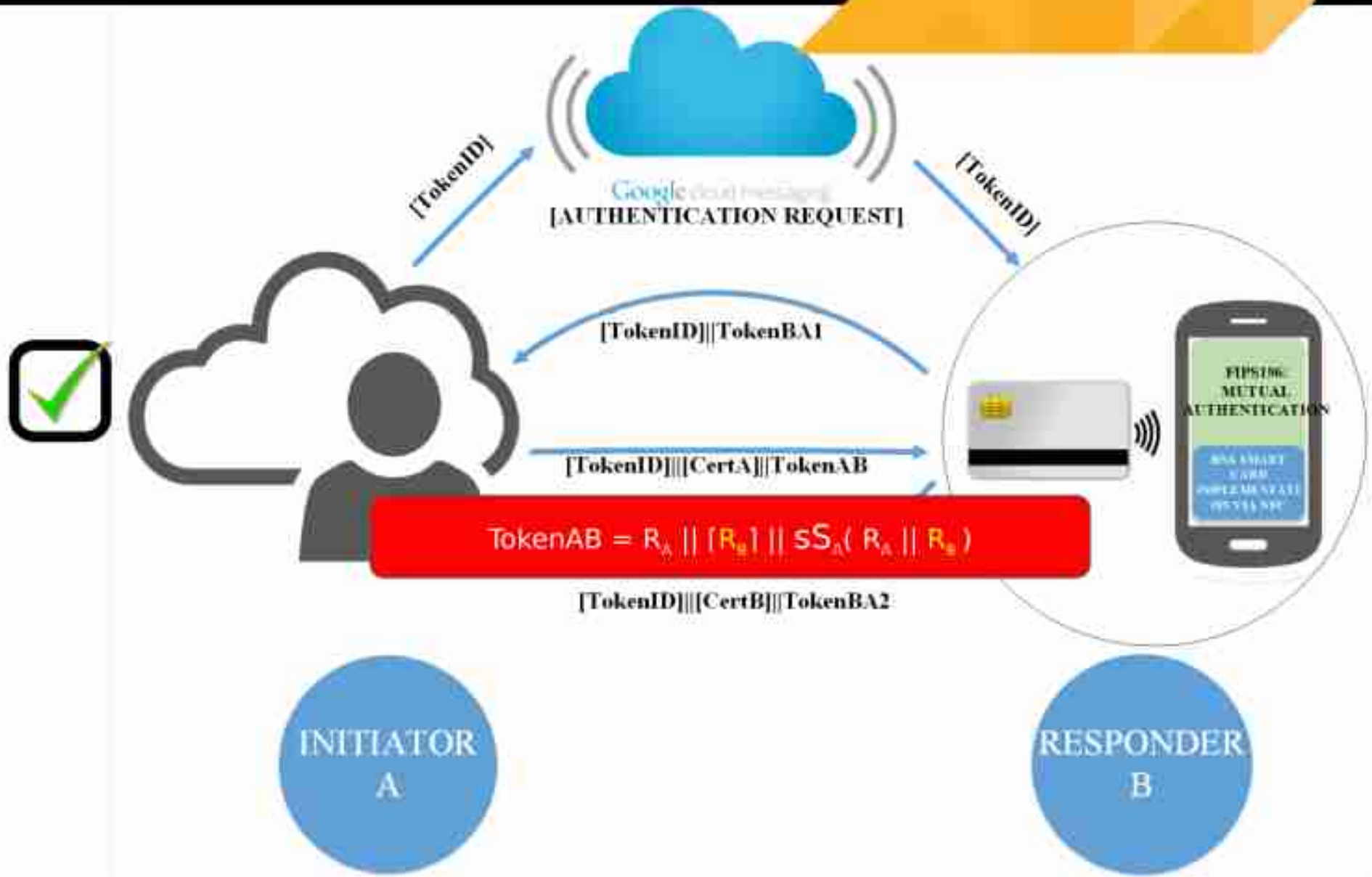
FIPS196 ON WEB



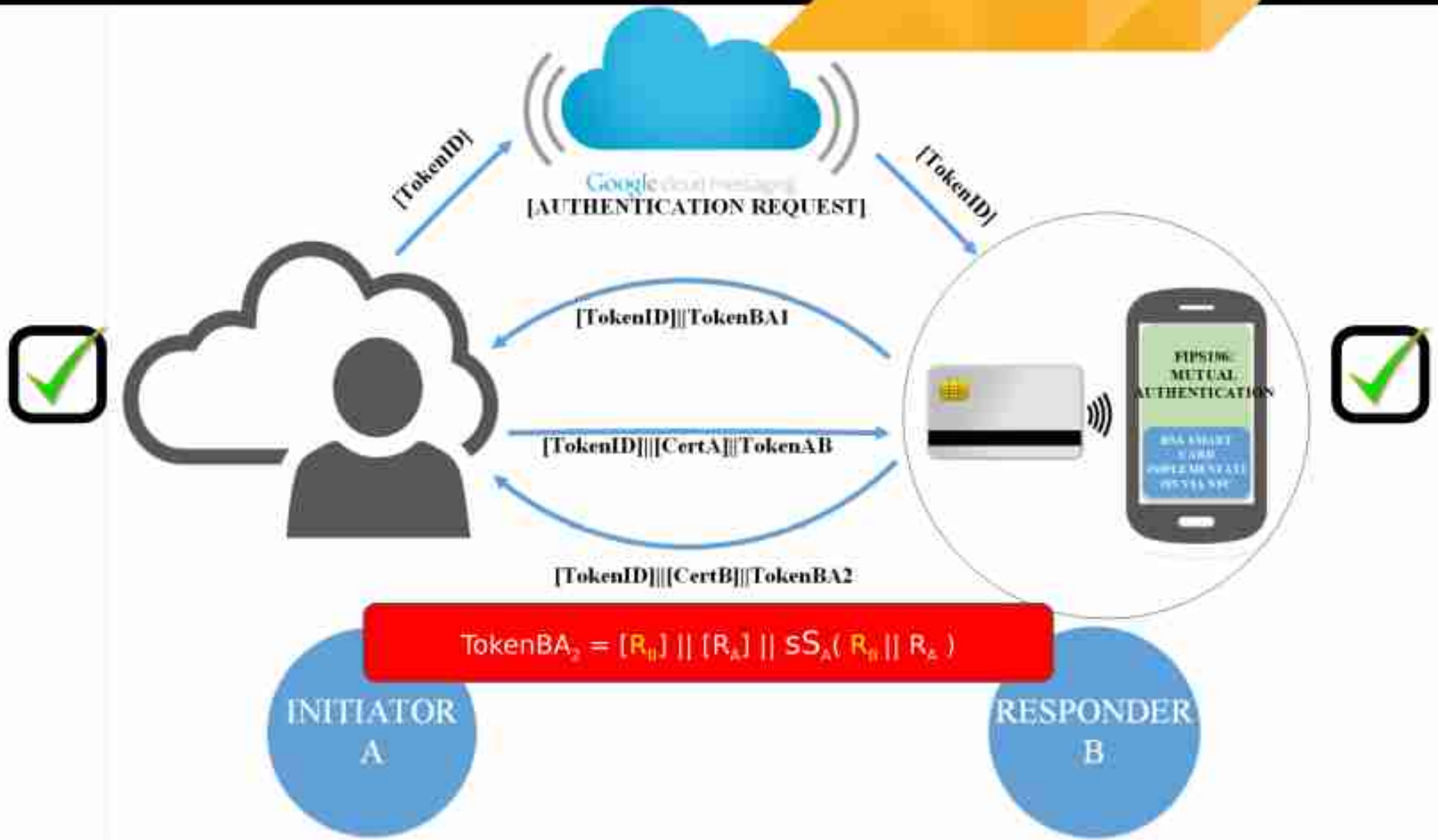
FIPS196 ON WEB

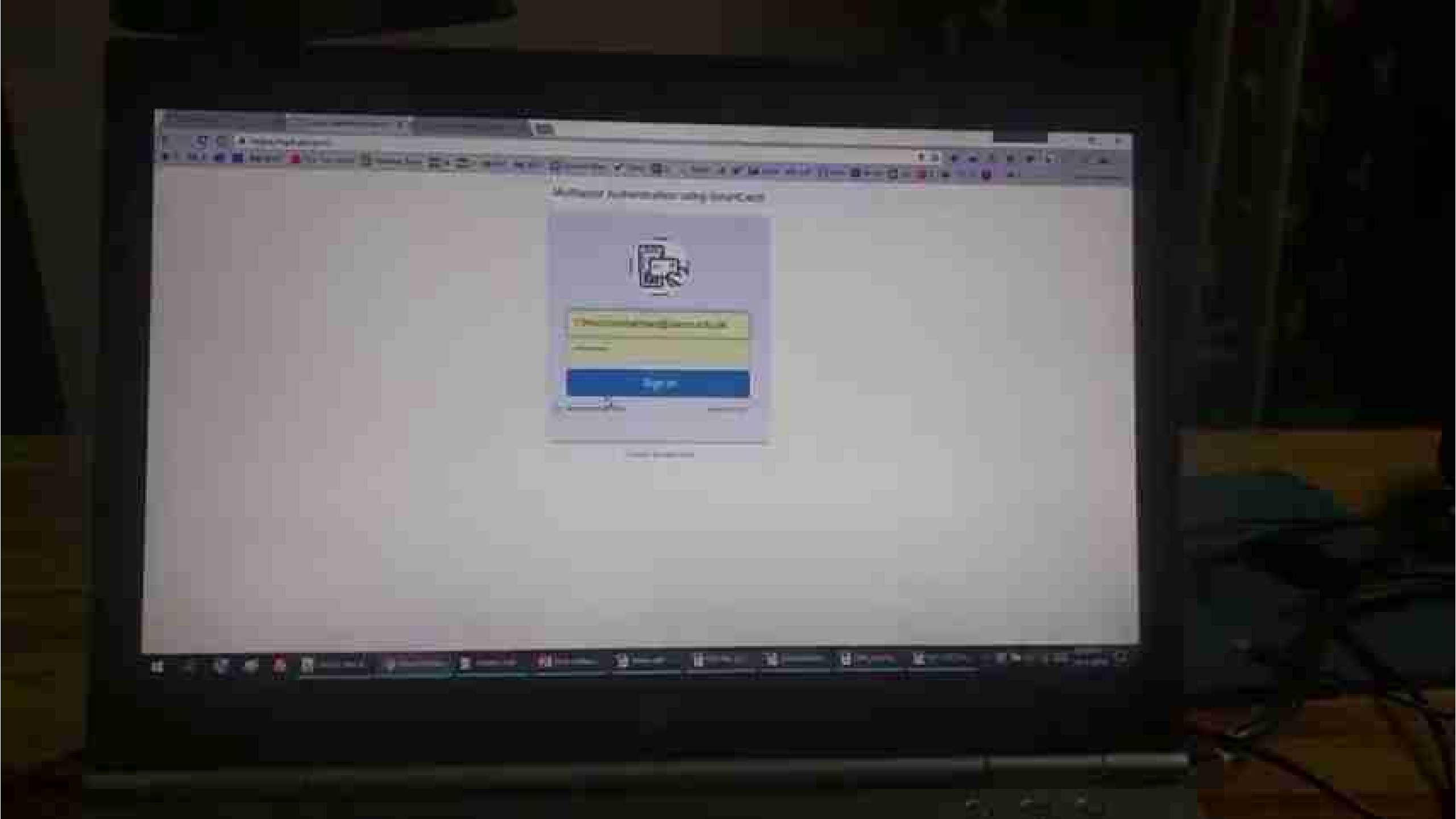


FIPS196 ON WEB



FIPS196 ON WEB





```
root@Securage:/opt/avispa-1.1/contrib# avispa smartauth.hlpsl --ofmc
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /opt/avispa-1.1/testsuite/results/smartauth.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.42s
  visitedNodes: 578 nodes
  depth: 10 plies
root@Securage:/opt/avispa-1.1/contrib#
```

AVISPA

SECURITY ANALYSIS

Security	Defense
Mutual Entity Verification	✅
Replay Attack Defense	✅
Man-in-the-middle attack Defense	✅
Phishing Attack Protection	✅

FUTURE WORK

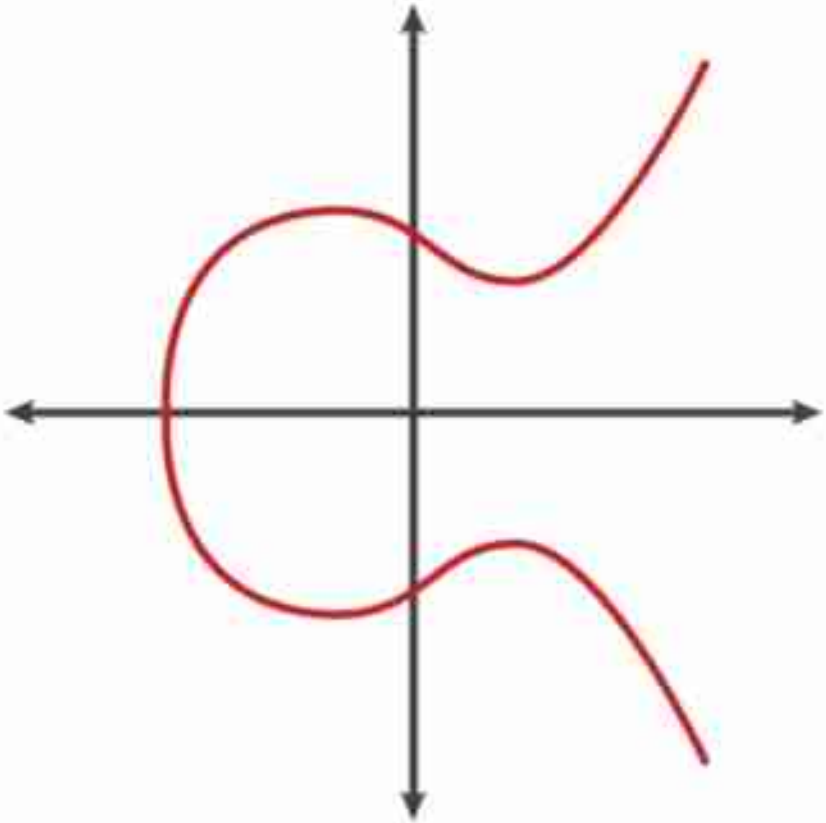
- **FIPS196 archived - October 19, 2015**

Latest revision - (February 18, 1997)

FUTURE WORK

Elliptic Curve Cryptography

ECC Key Size	RSA Security Equivalent
224 bit	2048 bit
256 bit	3072 bit
384 bit	7680 bit
521 bit	15360 bit

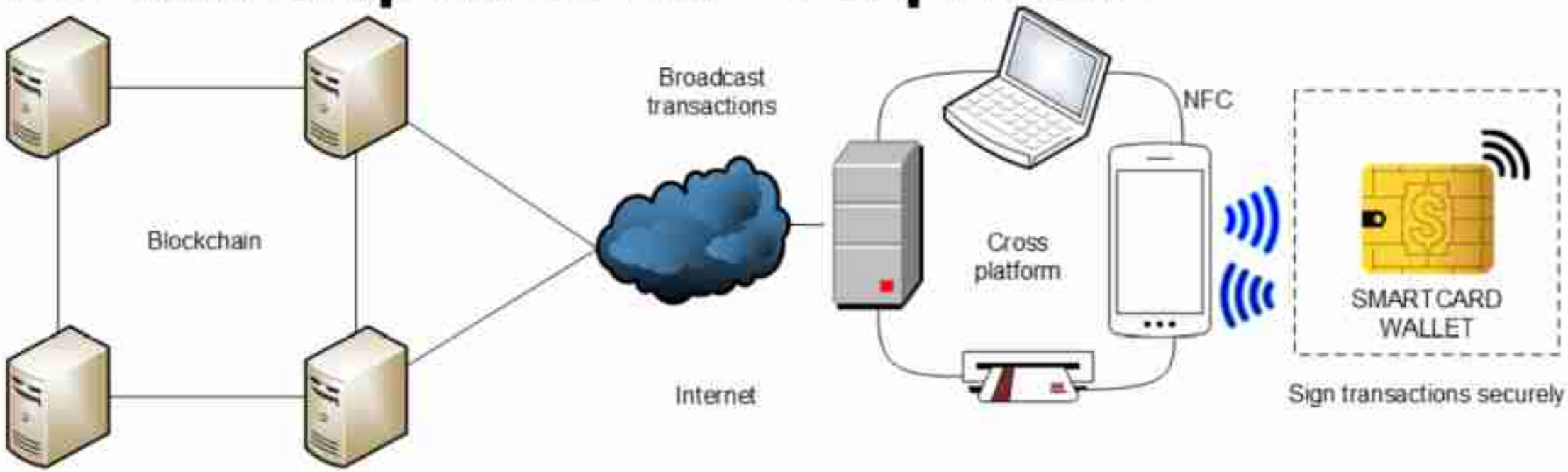


https://blog.gemalto.com/security/2015/01/27/elliptic-curve-cryptography-comes-of-age-small-keys-unlock-a-big-future/

https://blog.goodaudience.com/very-basic-elliptic-curve-cryptography-16c4f6c349ed

SMARTCARD WALLET

- **Bitcoin elliptic curve - Secp256k1**



AWARENESS

The first step to protecting yourself is to know the most common type of frauds.

Know the threat

Phishing

Phishing is where fraudsters send emails (often appearing to be from your bank) asking you to disclose personal information. Phishing emails will try to get you to download a file or click on a link to a bogus website, which may then allow fraudsters to access your confidential bank account or card details.

Voice + phishing = Vishing

Vishing is where fraudsters call you on your home or mobile phone, pretending to be a government official or someone from your bank, and ask you to validate your identity by sharing your confidential bank account or card details.

How you can protect yourself from different threats

Always

- ✓ Use a computer or device that you trust
- ✓ Log out after finishing an online banking session
- ✓ Clear the browser cache after each session so that your account information is removed from the device
- ✓ Keep your debit & credit card number & PINs secure

Never

- x Click on unknown links that look similar to Standard Chartered online banking. Any such email is a scam/fraud

REFERENCES

[1] CNET, "Android dominates 81 percent of world smartphone market," May 2014, accessed 18 5 2014. [Online]. Available: http://www.cnet.com/news/android-dominates-81-percent-of-world-smartphone-market/

[2] IDC, "Worldwide quarterly mobile phone tracker," accessed 18 5 2014. [Online]. Available: http://www.idc.com/tracker/showproductinfo.jsp?prod_id=37

[3] G. Inc., "Google," accessed 19 5 2014. [Online]. Available: https://www.google.com

[4] Softei, "Dual interface smart card," accessed 09 2 2016. [Online]. Available: http://www.softei.com/

[5] W. Effing, *Smart card handbook*. John Wiley & Sons, 2010.

[6] S. C. Alliance, "Smart card technology faq," accessed 11 02 2016. [Online]. Available: http://www.smartcardalliance.org/smart-cards-faq/

[7] S. Almuairfi, P. Veeraraghavan, and N. Chilamkurti, "Ipsc: implicit password authentication system," in *Advanced Information Networking and Applications (WAINA), 2011 IEEE Workshops of International Conference on*. IEEE, 2011, pp. 430–435.

[8] A. P. Sabevne and A. Stavrou, "Universal multi-factor authentication using graphical passwords," in *Signal Image Technology and Internet Based Systems, 2008. SITIS'08. IEEE International Conference on*. IEEE, 2008, pp. 625–632.

[9] P. F. II. Schneider, "Something you know, have, or are," accessed 16 02 2016. [Online]. Available: https://www.cs.cornell.edu/courses/cs513/2005fa/nnabanthpeople.html

[10] G. A. Miller, "The magical number seven, plus or minus two: some limits on our capacity for processing information." *Psychological review*, vol. 63, no. 2, p. 81, 1956.

[11] B. Schlegl-Bader and J. Sametinger, "Secure and usable authentication on mobile devices," in *Proceedings of the 10th International Conference on Advances in Mobile Computing & Multimedia*. ACM, 2012, pp. 257–262.

[12] J. Bonneau, "The science of guessing: analyzing an anonymized corpus of 70 million passwords," in *Security and Privacy (SP), 2012 IEEE Symposium on*. IEEE, 2012, pp. 538–552.

[13] M. J. Quinn, "Analysis of real-world passwords for social media sites," 2015.

[14] H.-M. Sun, Y.-H. Chen, and Y.-H. Lin, "tpass: A time authentication protocol resistant to password stealing and password reuse attacks," *Information Forensics and Security, IEEE Transactions on*, vol. 7, no. 2, pp. 651–663, 2012.

[15] D. Florencio and C. Herley, "A large-scale study of web password habits," in *Proceedings of the 16th international conference on World Wide Web*. ACM, 2007, pp. 657–666.

[16] "British airways frequent-flyer accounts hacked," accessed 17-02-2016. [Online]. Available: http://www.theguardian.com/business/2015/mar/20/british-airways-frequent-flyer-accounts-hacked

[17] "ebay suffers massive security breach, all users must change their passwords," accessed 17 02 2016. [Online]. Available: http://www.forbes.com/sites/gordonkelly/2014/05/21/ebay-suffers-massive-security-breach-all-users-must-their-change-passwords/#1c1581a63c15

[18] "icloud not compromised in apple id attack: Apple." [Online]. Available: http://www.zdnet.com/article/icloud-not-compromised-in-apple-id-attack-apple/

[21] A. De Luca, E. Von Zezschwitz, N. D. H. Nguyen, M.-E. Maurer, E. Rubegni, M. P. Scipioni, and M. Langheinrich, "Back-of-device authentication on smartphones," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2013, pp. 2389–2398.

[22] T. Vidas, D. Votipka, and N. Christin, "All your droid are belong to us: A survey of current android attacks." in *WOOT*, 2011, pp. 81–90.

[23] G. Inc., "Dashboards," accessed 27 2 2016. [Online]. Available: http://developer.android.com/about/dashboards/index.html

[24] ——, "Android," accessed 19 5 2014. [Online]. Available: http://www.android.com/

[25] G. Inc., "Introduction to android," accessed 19 5 2014. [Online]. Available: http://developer.android.com/guide/index.html

[26] ——, "Application fundamentals," accessed 19 5 2014. [Online]. Available: http://developer.android.com/guide/components/fundamentals.html

[27] G. Inc, "Android debug bridge," accessed 20 5 2014. [Online]. Available: http://developer.android.com/tools/help/adb.html

[28] G. Inc., "Near field communication," accessed 22 May 2015. [Online]. Available: https://developer.android.com/guide/topics/connectivity/nfc/nfc.html

[29] ——, "Advanced nfc," accessed 22 May 2015. [Online]. Available: https://developer.android.com/guide/topics/connectivity/nfc/advanced-nfc.html#tag-tech

[30] GlobalPlatform, "Globalplatform," accessed 02 3 2016. [Online]. Available: http://www.globalplatform.org/

[31] Z. Chen, *Java card technology for smart cards: architecture and programmer's guide*. Addison-Wesley Professional, 2000.

[32] G. Barthe, G. Dufay, L. Jakubiec, B. Serpette, and S. M. De Sousa, "A formal executable semantics of the javacard platform," in *ESOP*, vol. 1. Springer, 2001, pp. 302–319.

THANK YOU!


@M_Shahbaz_A


https://www.linkedin.com/in/mr-muhammad-shahbaz/


mr.shahbaz.aslam@gmail.com