



# **Password Less Authentication**

**(PLA)**

**Srikar Sagi**

# Agenda



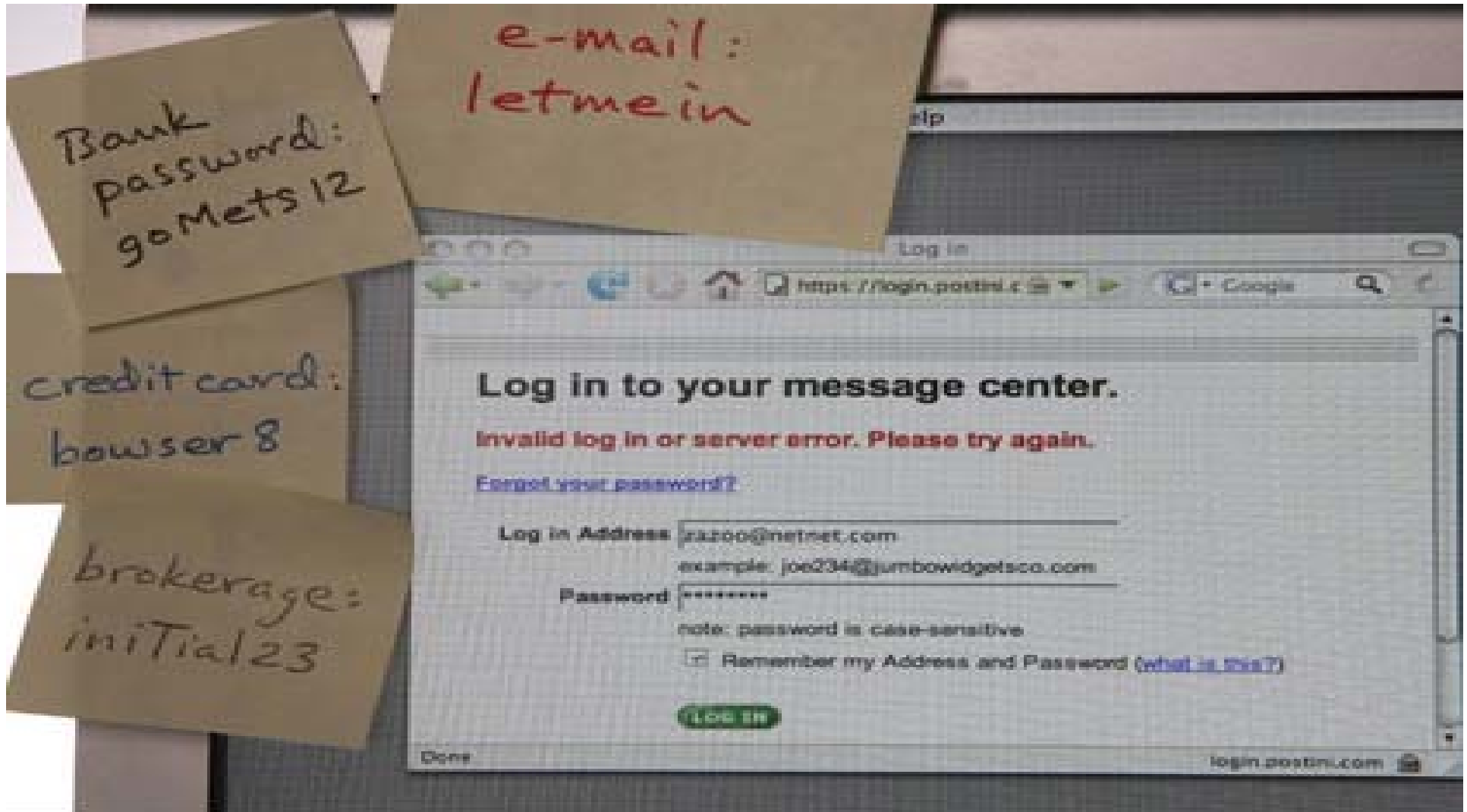
- Why Factors - Problem Statement**
- Why Factors - Motivations**
- Mobile Device based Authentication**
- User Registration**
- User Experience**
- Authentication Process**
- Authentication Schematics**
- Competitors to PLA**
- OTP & PLA Differentiators**
- References & QnA**
- Appendix**

# Why Factors-Problem Statements



## Customers

Too Many Passwords, password complexities, same passwords, sharing of passwords



# Why Factors-Problem Statements



## Customers

Password Changes, Reset requests & Remembering Security Questions for many sites

### Reset Password

New Password

Confirm Password

New Question

New Answer

### The password must meet the following requirements:

- ✓ Must contain at least 8 characters
- ✓ Must contain at least 1 uppercase letter
- ✓ Must contain at least 1 lowercase letter
- ✓ Must contain at least 1 digit
- ✓ Must contain at least 1 special character
- ✓ Must not contain any part of your username
- Must not repeat any of your previous 24 passwords
- Must differ from your previous password by more than the last character

Generate Password

Reset Password

Send Password

# Why Factors-Problem Statements



## Customers

Too many Tokens, Token Costs, Lost Tokens, Dispatch Costs & Lost Business Costs



# Why Factors-Problem Statements



## Executive Management

- Cost of -- Fraud Operations, Software Security Controls, Service Desk, Frustrated Users & Lost business
- Identity Theft 9.8% (IC3-2010) - 3rd Most Internet Crime  
[http://ic3report.nw3c.org/docs/2010\\_IC3\\_Report\\_02\\_10\\_11\\_low\\_res.pdf](http://ic3report.nw3c.org/docs/2010_IC3_Report_02_10_11_low_res.pdf)
- Ponemon Report - 2011 - Cost of Cyber Crime Study  
[http://docs.media.bitpipe.com/io\\_10x/io\\_101711/item\\_452026/2011%202nd%20Annual%20Ponemon%20Cost%20of%20Cybercrime%20Study.pdf](http://docs.media.bitpipe.com/io_10x/io_101711/item_452026/2011%202nd%20Annual%20Ponemon%20Cost%20of%20Cybercrime%20Study.pdf)
- The Shocking Scale of Cybercrime - Shared by Richard R. in Mobile Security Trends - LinkedIn  
[http://www.linkedin.com/news?viewArticle=&articleID=761361820&gid=3802786&type=member&item=69965873&articleURL=http%3A%2F%2Fus.norton.com%2Fcontent%2Fen%2Fus%2Fhome\\_homeoffice%2Fhtml%2Fcybercrimereport%2F&urlhash=Cjo1&goback=.gde\\_3802786\\_member\\_69965873](http://www.linkedin.com/news?viewArticle=&articleID=761361820&gid=3802786&type=member&item=69965873&articleURL=http%3A%2F%2Fus.norton.com%2Fcontent%2Fen%2Fus%2Fhome_homeoffice%2Fhtml%2Fcybercrimereport%2F&urlhash=Cjo1&goback=.gde_3802786_member_69965873)
- State of Enterprise Security - 2010 Report by Norton  
[http://www.symantec.com/content/en/us/about/presskits/SES\\_report\\_Feb2010.pdf](http://www.symantec.com/content/en/us/about/presskits/SES_report_Feb2010.pdf)



# Why Factors-Motivation



## SMS Bank Tokens Vulnerable

<http://www.zdnet.com.au/sms-bank-tokens-vulnerable-rsa-339308633.htm>

ZDNet / Security / Story

## SMS bank tokens vulnerable: RSA

By Darren Pauli, ZDNet.com.au on January 18th, 2011

**Mobile phone attacks will increase this year as criminals attempt to intercept SMS-based authentication tokens, according to security company RSA.**

The tokens are designed to complement username and password log-in checks by requiring users to validate payments with unique numerical codes, in this instance sent by SMS.

It is becoming more popular, and the Commonwealth Bank of Australia claims to have 80 per cent of its customer base using tokens to validate third-party payments via SMS or through safer handheld token-number generators. The bank isn't forcing customers to use it, but those who don't will not be permitted to carry out high-risk transactions over NetBank.



*(iPhone 4 image by Jorge Quinteros, CC2.0)*

RSA said in a 2011 predictions report that sending tokens via SMS will make phones a target.

"The use of out-of-band authentication SMS ... as an additional layer of security adds to the vulnerabilities in the mobile channel," the company said in its report.

"A criminal can ... conduct a telephony denial-of-service attack which essentially renders a consumer's mobile device unavailable.

"SMS forwarding services are also becoming mainstream in the fraud underground and enable the [token] sent by a bank via text to a user's mobile phone to be intercepted and forwarded directly to the cyber criminal's phone."

The company said that mobile phone smishing attacks, or phishing scams sent via SMS, will also rise this year.

# Why Factors-Motivation



One Time Passwords are not Secure – Analysis

<https://infosecisland.com/blogview/11813-One-Time-Passwords-are-Not-Secure-Enough.html>

<http://www.nowires.org/Papers-PDF/OTPanalysis.pdf>



[Front Page](#) | [Blog Posts](#) | [Downloads](#) | [Videos](#) | [From the Web](#) | [Forums](#) | [Free Tools](#) | [Breaches](#) |

## One Time Passwords are Not Secure Enough

Monday, February 14, 2011

Contributed By:  
**Gurudatt Shenoy**



### The thing About One Time Passwords... It is Not Secure Enough

An OTP, or One Time Password, is becoming quite a fashion these days. There are many ways to generate OTPs, and a swarm of security companies have sprung up, each offering a different variant of One Time Password technology.

This is not surprising, as even Google has awakened to the concept of OTP in securing users from phishing attacks for Google Docs and other access points.

And the herd mentality follows.

No doubt, OTP-based two factor authentication is far more secure than single factor authentication and is also cheaper.

But, is it really secure enough to thwart the efforts of dedicated hackers who have broken into highly secured government and defense enterprises deploying even far more secured solutions?

I do not think so.

OTP is equally vulnerable because the action remains on the same device that the first layer of authentication occurs (username and password).

For example, if a victim's computer is already vulnerable to key-loggers and other malware that can track what the victim is keying-in, and also take action based on the



# Why Factors-Motivation



## RSA Secure-ID Hardware Token Hacked

<http://technorati.com/technology/it/article/rsa-hackedtime-to-panic-for-corporate/>



Home / Technology / IT / Articles / RSA Hacked—Time to Panic For Corporate I.T.?

## RSA Hacked—Time to Panic For Corporate I.T.?

Author: James Cohen

Published: March 18, 2011 at 2:18 pm

Share

Network security vendor RSA has announced that they have been the victim of "an extremely sophisticated cyber attack in progress being mounted against RSA". Specific details of the breach have been limited thus far, but RSA has confirmed that data taken from their network directly pertains to their SecurID two factor authentication products.



The SecurID system is employed by corporations and businesses all over the world as a means of securing access to sensitive business systems both on-site and from remote locations. The keys generated by the system require a user to connect using their username, a personalized PIN number, and a security token generated by SecureID devices. Each token is generated by the user when they begin a connection, and usually remains valid for about 30 seconds. This method has been a cornerstone of system access security for quite some time, but now may be at risk of breach.

If you've never seen a SecurID device, they typically appear as a keychain sized box with a small LCD screen that allows an individual the ability to generate personal access codes on demand to connect to business systems. The breach at RSA, while not directly jeopardizing any consumer data, could lead to subsequent attacks on systems that use the device for security.

RSA chairman Arthur W. Coviello Jr. posted an open letter on the company's website detailing the steps that RSA is taking to mitigate the damage. Unfortunately, at this stage, SecurID customers are forced to rely on their employees to take appropriate steps to safeguard their access information. It's safe to say that currently nobody knows how or when the hackers will attempt to use the stolen data, but it's likely they will try.

# Why Factors-Motivation



US Chamber of Commerce – Proposing No Passwords, Only H/W or Smart Phone based Login

<http://arstechnica.com/tech-policy/news/2011/04/with-passwords-broken-us-rolls-out-internet-identity-plan.ars>

› Law & Disorder

☛ Tech law and policy in the digital age



## With passwords "broken," US rolls out Internet identity plan

By Nate Anderson | Published April 15, 2011 12:05 PM



At a US Chamber of Commerce event today, the federal government rolled out its vision for robust online credentials that it hopes will replace the current mess of multiple accounts and insecure passwords. The choice of the Chamber of Commerce wasn't an accident, either; the government wants to squelch any talk of a "national Internet ID card" and emphasize that the plan will be both voluntary and led by the private sector.

The **National Strategy for Trusted Identities in Cyberspace** (NSTIC) hasn't changed much since the **draft plan unveiled in January**, though the **final version** (PDF) contains an even stronger emphasis on NSTIC being a private-sector, voluntary undertaking. This point was stressed so many times in a background briefing call for reporters this morning that it's clear the government fears a potential backlash against its efforts.

The final version of NSTIC tries to address two problems: the fact that passwords are "broken" and the fact that it's almost impossible to prove your identity on the Internet. The future belongs to smart cards, cell phones, USB security sticks, and similar solutions—when the Department of Defense moved away from passwords to a smartcard security solution, it saw network intrusions drop by 46 percent.

The rest of the system is simpler, says the briefing notes, needed for online consumers to check out their...

# Why Factors-Motivation



- Human *Psyche* for Mobile phones**
- Frustrated Users – many & similar Passwords**
- Human Dependency on Mobile phones**
- Trust on Mobile Network's Control Channel**
- Increase in Mobile Device Capabilities**
- Use of Mobile's Geo Loc' for Authorization Decision**
- Trust on Public Key Cryptography**
- Automated Mobile Signal attacks are costly (Logistics)**
- Mobile Apps – Controlled by Central Release Authorities**
- Mobile Phone Population crossing 5 Billion devices**
- Adult(15-65)Population more than 3 Billion out of 7 Billion**
- Expected – 50 Billion Internet connected Devices by 2020**

# Mobile Device based Authentication



## Ownership Based Authentication with Mobile

For

1. Speed of Auth/Z
2. Ease of Use (UI, Registration)
3. Adaptation Flexibility & Scalability

# User Registration



**Account login**

User Name

Password

Go to

**Log In**

[Problem with login?](#)

**PLA Authentication**

User Id

PIN

**Request Challenge-1**

New to PLA? [Register](#)

# User Registration

## FaceLog Payments & Identity Systems

Welcome Nikolas

-----I Want Password Less Authentication-----

Last log in March 13, 2011 11:26 PM PDT

Account Type: Premier | Status: [verified](#)

Difficult to remember all your passwords??Here is a boon for it!!!!Just remember one pin and forget all your password's!!!Click on me to try!!!

Available balance in USD (primary): \$1,042.90 USD

Total balance (all currencies, available and pending) converted to USD: \$5,074.65 USD [Hide](#)

Currency	Total
USD (Primary)	\$1,042.90 USD
CAD	\$1,712.10 CAD
GBP	£604.50 GBP
EUR	€560.50 EUR
AUD	\$386.10 AUD

[See all balances](#)

[Accept payment](#)

[Update my credit card info](#)

[Policy Updates](#)

My recent activity | [Payments received](#) | [Payments sent](#)

[View all of my transactions](#)

# User Registration



## FaceLog Payments & Identity Systems

### Registration for Password Less Authentication

User Name

**nikolas@facelog.com**

Choose a 6 Digit PIN

(The same PIN you need to select for your mobile Application)

**123789**

Re-Enter Same 6 Digit PIN

(The same PIN you need to select for your mobile Application)

**123789**

Enter Personal Mobile Phone Number (This Mobile Proves Your Identity – Hence Keep this Phone Private to yourself)

(Eg: If your mobile Number is 9647748443 and your country is India then enter as 919647748443)

**919176617699**

Re-Enter Personal Mobile Phone Number (This Mobile Proves Your Identity – Hence Keep this Phone Private to yourself)

(Eg: If your mobile Number is 9647748443 and your country is India then enter as 919647748443)

**919176617699**

**Your Download Message Code = X12-972JM123-ABC – Download the app only if you see this**

**I Agree All Terms & Conditions & Register me for PLA**

# User Registration

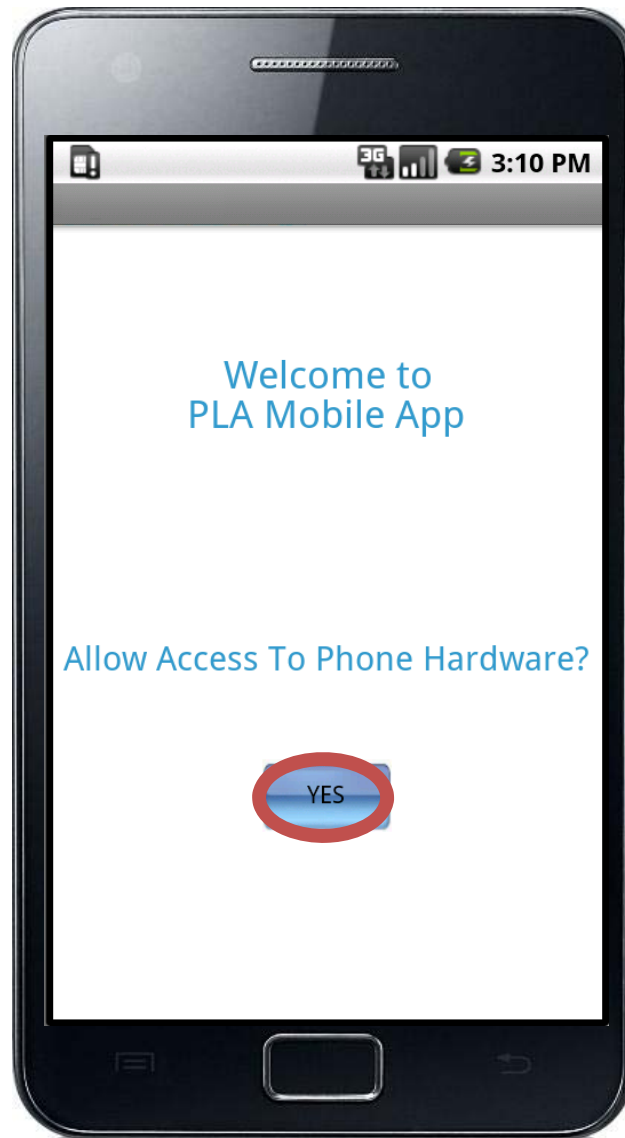




# User Registration

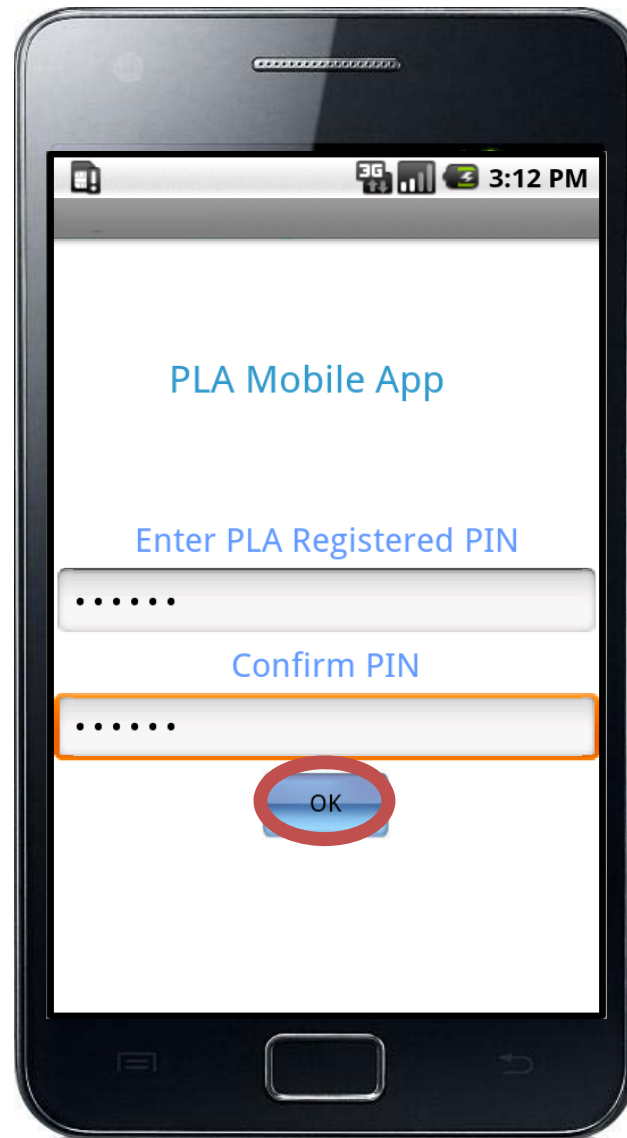


# User Registration



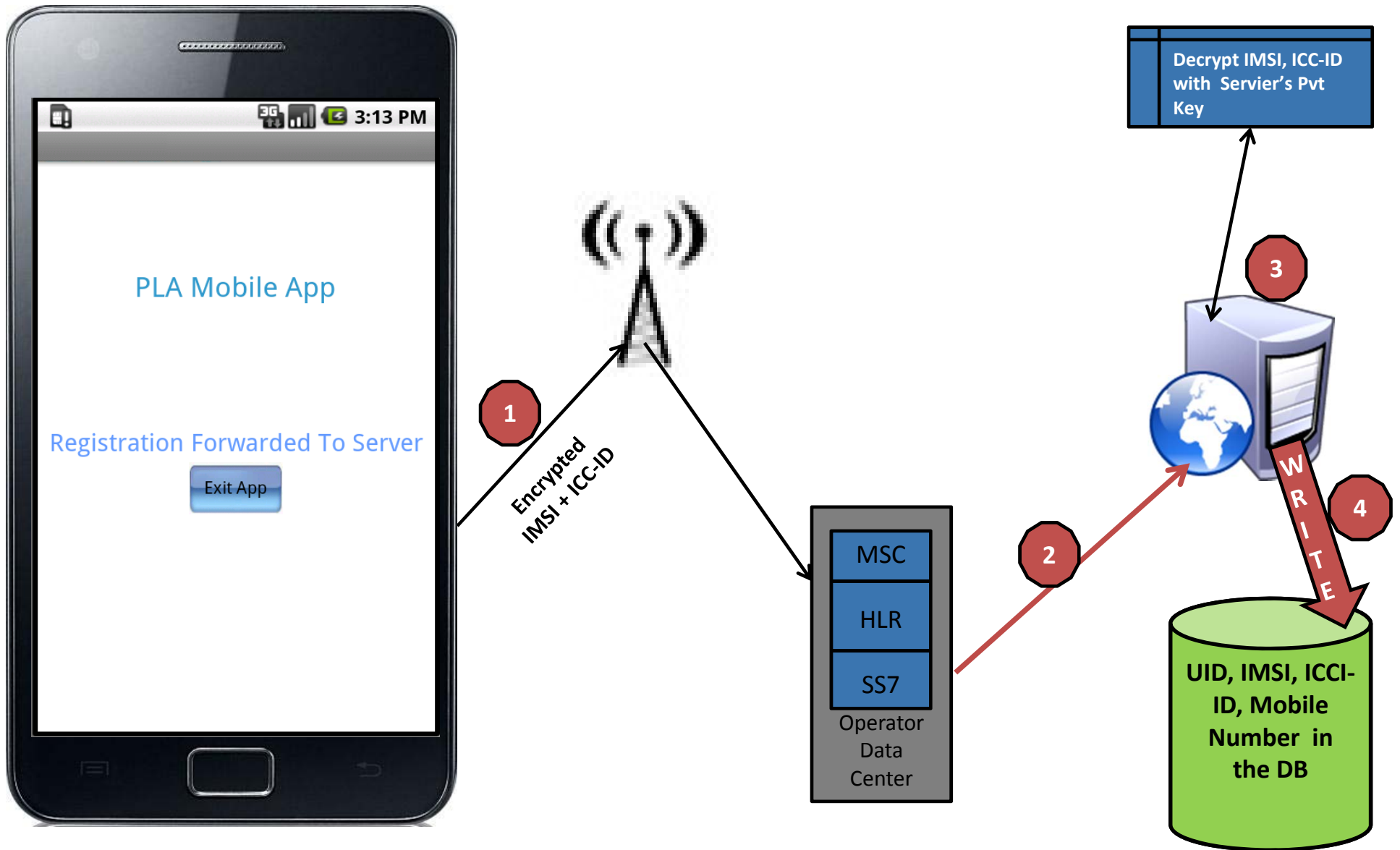
To read  
IMSI &  
ICC-ID

# User Registration

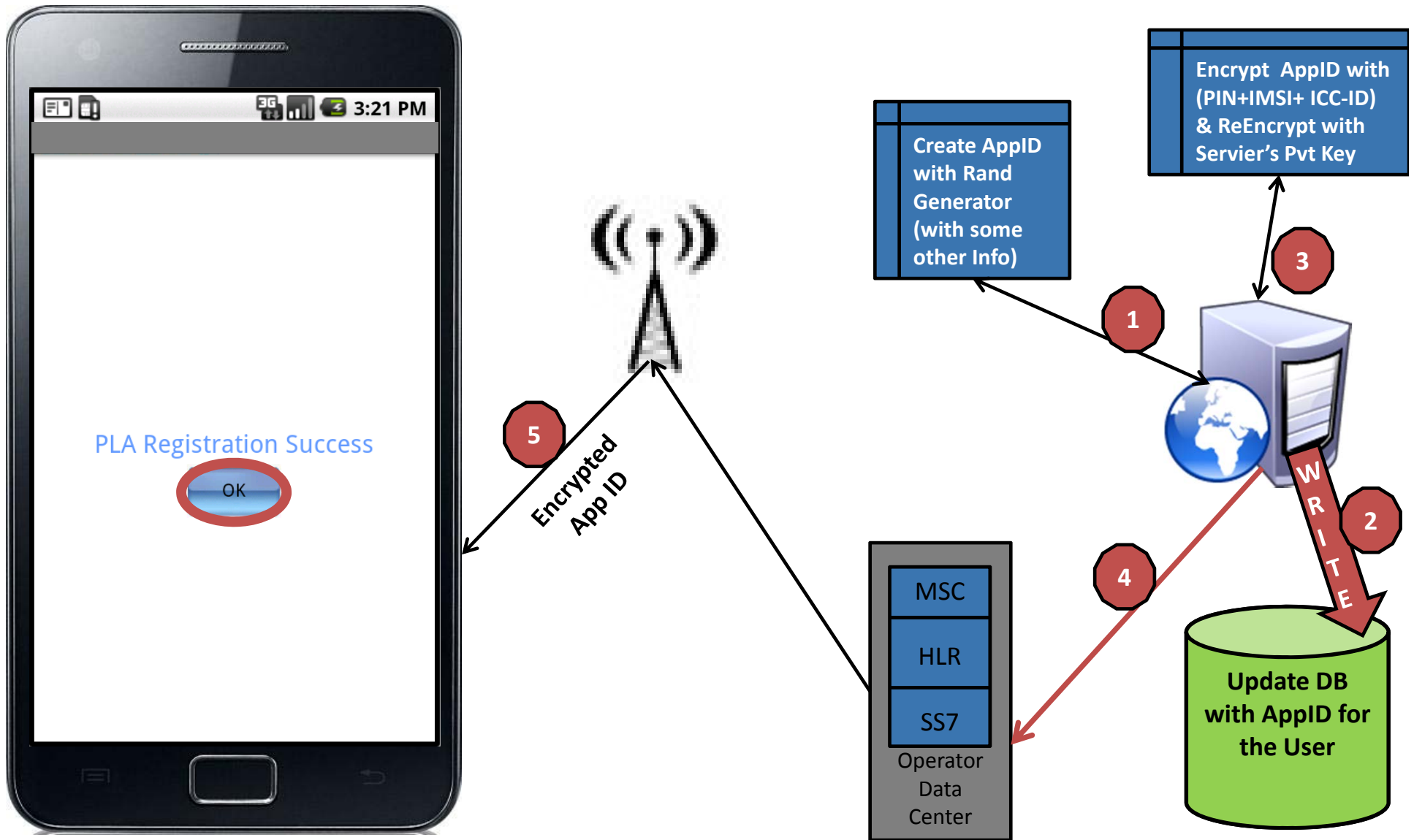


Same PIN  
Entered on  
the web page

# User Registration



# User Registration





## FaceLog Payments & Identity Systems

Account login

User Name

Password

Go to  
My account

[Problem with login?](#)

PLA Authentication

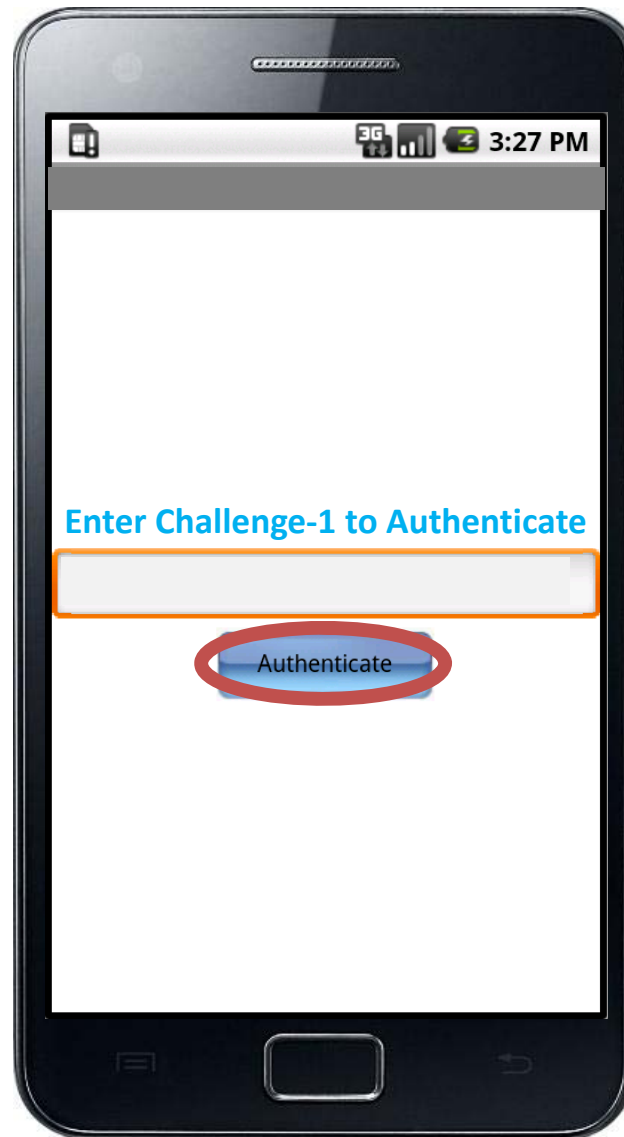
User Id

PIN

**Request Challenge-1**

**Your Web Challenge  
Enter This Challenge  
in Your Mobile App  
5678**







## FaceLog Payments & Identity Systems

[Overview](#) [Add Funds](#) [Withdraw](#) [History](#) [Resolution Center](#) [Profile](#)

**Welcome Nikolas**  
**Authentication Success!!**

Account Type: Premier | Status: Verified

**You have logged in on, 8/10/2011 12.34 pm**

From IP address: 10.239.41.48



# Authentication Process



- Step-1** Credential Collection on ***TWO distinct*** Networks
- Step-2** User ID is sent by User as ***multipart/x-mixed-replace*** Request and ***Challenge-1*** is received on Web Page from Server on IP Network as a multipart/x-mixed-replace Response
- Step-3** Server Sends ***Challenge-2*** as Push/SMS Message on Mobile Phone over the air using Telecom Network (stores Challenge-1 & 2)
- Step-4** User enters ***Challenge-1*** on Mobile App & Mobile App reads ***Challenge-2*** from Push/SMS, Hashes ***C1+C2+IMSI+ICC-ID+AppID*** and Encrypts with Server's Public Key (Encrypted Packet)
- NOTE:** ***Challenge-2*** is always Opaque to user– may or may not know

# Authentication Process



**Step-5** Encrypted Packet is Sent as SMS/Push Response from Mobile Network

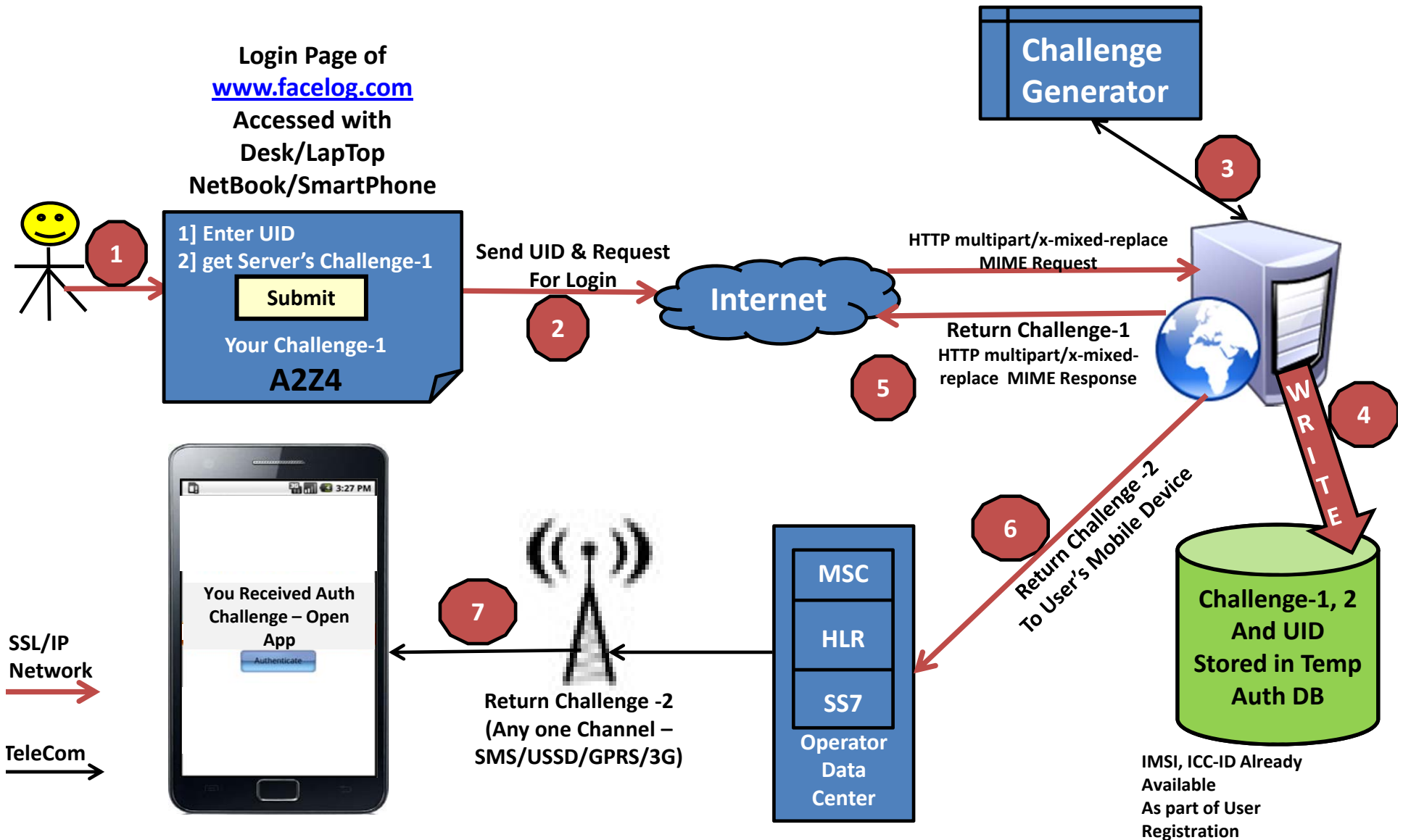
**Step-6** Server reads the Push Response/SMS Message from User

**Step-7** Server Decrypts Encrypted Packet with its Private Key

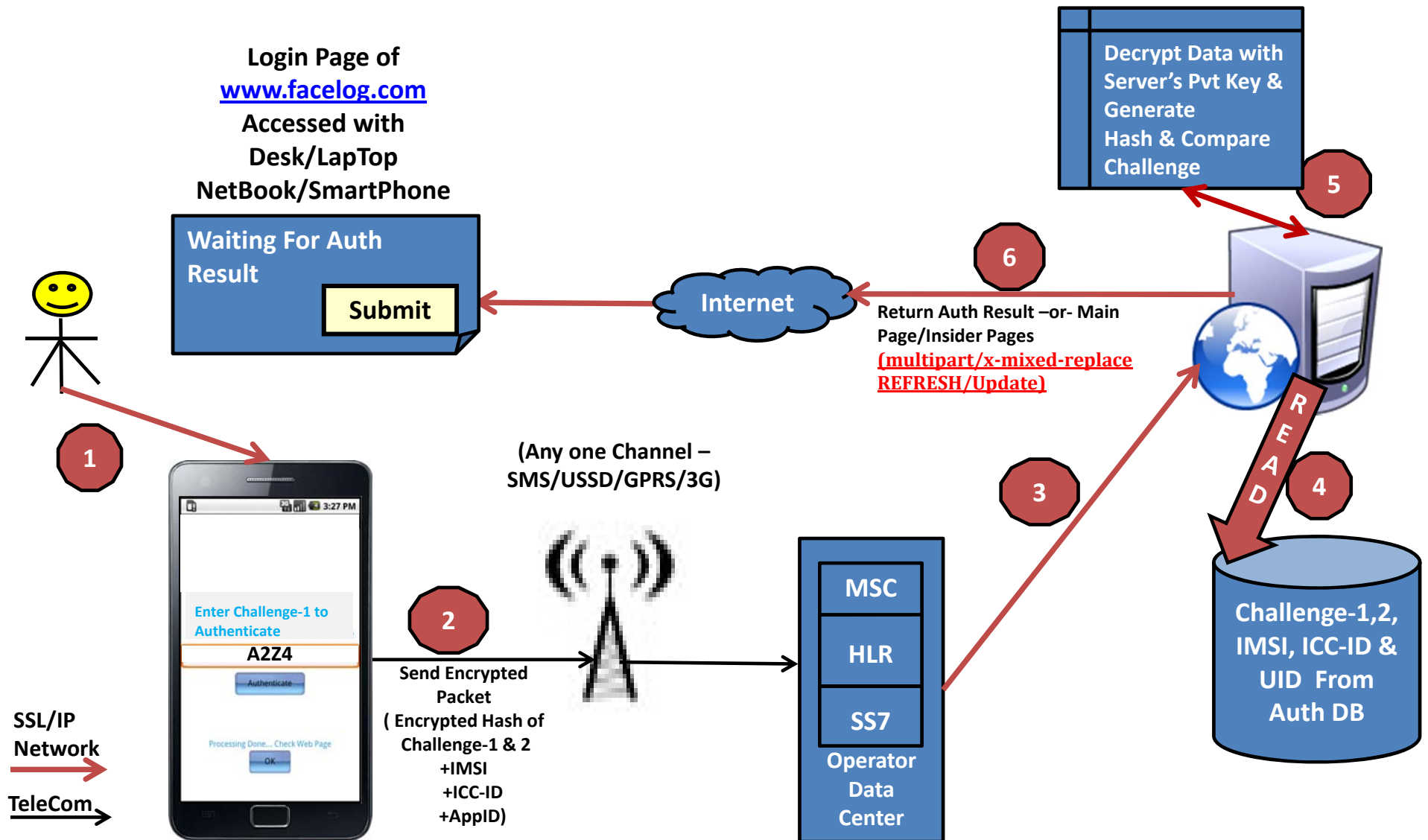
**Step-8** Server loads ***C1+C2+IMSI+ICC-ID+AppID*** stored in the Database for that user's request and hashes again

**Step-9** If Hashes Match then Welcome screen is pushed to the web user as a Response to ***multipart/x-mixed-replace***

# Authentication Schematics



# Authentication Schematics



# Best Channel – Real Experience for PLA



#	Connectivity Protocol / Bearer Channel	Dev Cost	OS Comp	Initial Testing Cost	Integration Cost (Between Operator & Servers)	Connection Speed	Connection Type	Location Dependency	User Experience (Server Response Speed)	Setup Costs (H/W & S/W)	End User Charges	OPS Cost	Support (user compliant)
1	SMS	LOW	Devices that has Java 1.4 or above	MEDIUM	LOWEST	LOW	Store & Forward	Yes - LOW	LOW	LOW	LOW	MEDIUM	HIGH
2	GPRS	MEDIUM	Devices that has Java 1.4 or above	LOW	LOW	MEDIUM	Packet Based	Yes - LOW	SUPER	LOW	MEDIUM	MEDIUM	MEDIUM
3	3G	HIGH	Devices that has Java 1.4 or above	HIGH	HIGH	HIGH	Conn--Oriented	Yes - HIGH	SUPERLATIVE	HIGH	HIGH	HIGH	HIGH
<b>Best Channel with Best User Experience</b>													
4	USSD- USSR Over SMPP	LOW	Devices that has Java 1.4 or above	HIGH	HIGH	HIGH	Session based (between Handset & N/W)	Yes - HIGH	SUPERLATIVE	MEDIUM	NIL	LOW	MEDIUM

USSR-Unstructured Supplementary Service Request (Network Initiated Push for Application Start-Up)

# Competitors to PLA



## Products –

Browser ID

Solid Pass.com (All or some products)

Google PIN Check/Verification Code

## Research Papers –

Secure Web Authentication with Mobile Phones by Min Wu, Simson Garfinkel, Rob Miller @ M.I.T

<http://homepages.mcs.vuw.ac.nz/~ian/shared/papers/secureweb.pdf>

Secure Web Authentication with Mobile Phones by Min Wu, Simson Garfinkel, Rob Miller @ M.I.T

<http://dimacs.rutgers.edu/Workshops/Tools/slides/wu.ppt>

The same paper that was published in IEEE

[http://ieeexplore.ieee.org/xpl/freeabs\\_all.jsp?arnumber=5951918](http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=5951918)

**PLA**, Browser ID, Solid Pass & Google PIN Check & the research paper by MIT Students all are based on “**Ownership**” based authentication model and hence they all can be directly compared for

1. Speed of Auth/Z
2. Ease of Use (UI, Registration)
3. Portability
4. Adaptation Flexibility & Scalability
5. Security Aspects

# OTP & PLA - Differentiators



## OTPs

- 1 Multiple Tokens - for each "Secure Banking Service" - ICICI, HDFC, CITI
- 2 Remember UIDs or User Nos
- 3 Remembering respective passwords for each User IDs or User Numbers
- 4 Changing respective passwords for each User IDs or User Numbers in Credential life cycle
- 5 Dependent on Mobile Network  
**(Mobile OTPs & PLA Both)**
- 6 Cost for HelpDesk/Support Calls for  
Login Issues/Resets  
Token Issuance, Maintenance  
Token Support calls

## PLA

- No need to carry multiple tokens for each "Secure Banking Service"
- No remembering of passwords** for any "Secure Banking Service" - **Only remember the user ID**
- Easy to add new "Public Key" for any "Secure Banking Service" in same mobile app.
- Application Logic shall take care of selecting which "Public Key" to use to encrypt Tokens for which "Secure Banking Service"
- Can be used for "Authorization" as well (Requires additional development)
- Secure Banking Service can avoid the COSTS of**  
Login issues on the IP Network  
Password Strength/Expiry/Losses/Resets  
**Only Mobile App Updates is unavoidable cost**  
HelpDesk/Service Desk Calls

# References



- [1] Identity Theft 9.8% (IC3-2010) - 3rd Most Internet Crime  
[http://ic3report.nw3c.org/docs/2010\\_IC3\\_Report\\_02\\_10\\_11\\_low\\_res.pdf](http://ic3report.nw3c.org/docs/2010_IC3_Report_02_10_11_low_res.pdf)
- [2] Ponemon Report - 2011 - Cost of Cyber Crime Study  
[http://docs.media.bitpipe.com/io\\_10x/io\\_101711/item\\_452026/2011%202nd%20Annual%20Ponemon%20Cost%20of%20Cybercrime%20Study.pdf](http://docs.media.bitpipe.com/io_10x/io_101711/item_452026/2011%202nd%20Annual%20Ponemon%20Cost%20of%20Cybercrime%20Study.pdf)
- [3] SMS Bank Tokens Vulnerable  
<http://www.zdnet.com.au/sms-bank-tokens-vulnerable-rsa-339308633.htm>
- [4] One Time Passwords are not Secure - Analysis  
<https://infosecisland.com/blogview/11813-One-Time-Passwords-are-Not-Secure-Enough.html>  
<http://www.nowires.org/Papers-PDF/OTPanalysis.pdf>
- [5] RSA Secure-ID Hardware Token Hacked  
<http://technorati.com/technology/it/article/rsa-hackedtime-to-panic-for-corporate/>
- [6] US Chamber of Commerce - Proposing No Passwords, Only H/W or Smart Phone based Login  
<http://arstechnica.com/tech-policy/news/2011/04/with-passwords-broken-us-rolls-out-internet-identity-plan.ars>
- [7] Response time reasons & panic of users for their lost or stolen mobiles  
<http://www.zdnetasia.com/hardware-vulnerable-in-two-factor-authentication-39342580.htm>
- [8] Token Types, Costs, Comparisons & Current Implementors  
<http://www.zdnetasia.com/war-of-the-tokens-62037260.htm>
- [9] Miscellaneous  
<http://news.techworld.com/security/3258312/hackers-break-us-government-smart-card-security>  
<http://blogs.gartner.com/avivah-litan/2010/12/15/2011-threats-and-trends/>  
[http://www.bankinfosecurity.com/articles.php?art\\_id=1732](http://www.bankinfosecurity.com/articles.php?art_id=1732)  
[http://www.bankinfosecurity.com/articles.php?art\\_id=2728](http://www.bankinfosecurity.com/articles.php?art_id=2728)







# Appendix

- POC Exploit/Failure Scenarios**
- Differentiators - OTP & POC**
- OTP Costs & Cons**
- References**



## ❑ POC Exploit-1- Replay SMS attack

Attacker can replay i.e. Capture the signal & resend it within the time frame – attacker would only help the end user of the POC

## ❑ POC Exploit-2- Sending Fake SMS

Attacker can send fake SMS on behalf the POC User – but cannot receive SMS on behalf of POC User – Courtesy “**Control Channel**” of Mobile Network, for a successful authentication the attacker must receive the initial Push/SMS Message

## ❑ POC Exploit-3- A total Compromise

For Successful compromise attacker must know & have: User ID, Cell Phone No, IMSI, ICC-ID, Token-1 & 2, AppID and the “**Control Channel**” to receive Network Message



## ❑ POC Exploit-4- Lost/Stolen Mobiles

Mobile Phone is a precious device hence the time taken for an owner to discover loss of Mobile is likely to be much shorter compared to loss of tokens, which is used only while making a banking transaction.

----Jukka Riivari, CEO & President of Meridea

Source:

<http://www.zdnetasia.com/hardware-vulnerable-in-two-factor-authentication-39342580.htm>

## ❑ POC Exploit-5- Zero Protection Scenario

Attacker having overpowered the POC User & Mobile Subscriber, took control of Mobile device & the Desktop/Laptop/NetBook – this POC will completely fail

## ❑ POC Failure Scenario–1- Multiple Users

POC cannot be used in Least Developed Countries, where Micro-Payments are rampant for Multiple Users per mobile

# OTP Costs & Cons



## Hardware token

-Source -<http://www.zdnetasia.com/war-of-the-tokens-62037260.htm>

**Banks** ABN Amro, China Construction Bank, Citibank Singapore, DBS, HSBC, OCBC, UBS, UOB

- Pros**
- Has been around longer
  - Not dependent on the mobile phone operator network
  - Does not require any downloads or setup

- Cons**
- Inconvenience due to "necklace syndrome",  
-where customers with multiple Bank A/c with different Banks will have to carry multiple tokens
  - Higher implementation costs.
  - Experts estimate hardware's recurring costs to be around S\$40 (US\$24.50) to S\$60 (US\$36.74) per user per year, compared to under S\$10 (US\$6.12) per user per year for software-based tokens
  - Customer has to pay a replacement fee if it's lost
  - Not tamper-proof



## Software token for mobile

- Source- <http://www.zdnetasia.com/war-of-the-tokens-62037260.htm>

**Banks** OCBC Singapore

**Pros** - Mobile phone is ubiquitous

- No replacement fee; customer simply has to download the software application to his new phone

**Cons** - **Dependent on the mobile operator network**

- **Mobile phone can be as easily lost as hardware token, although chances of someone realizing his phone is missing are higher than it would be with the hardware token**

- **Still very new & customers are less familiar with process, compared to SMS**

# OTP Costs & Cons



## SMS Tokens

- Source - <http://www.zdnetasia.com/war-of-the-tokens-62037260.htm>

**Banks** Citibank Singapore & Hong Kong, OCBC, Standard Chartered, UOB

- Pros**
- Mobile phone is ubiquitous
  - People in Asia are familiar with SMS
  - Requires no training

- Cons**
- **Dependent on the mobile operator network**
  - **Potential issues like lost transmission and unexpected delay during festive seasons or when one is overseas**
  - **Mobile phone can be as easily lost as hardware token, although the chances of someone realizing his phone is missing are higher than it would be with the hardware token**