PKI and Applications (PKIA 2017)

Jagdeep S Kochar
“The most profound technologies are those that disappear.

They weave themselves into the fabric of everyday life until they are indistinguishable from it.”

— Mark Weiser, Chief scientist, Xerox, 1991
Internet Today

2017 This Is What Happens In An Internet Minute

- Facebook: 3.5 Million Logins
- Google: 900,000 Logins
- YouTube: 24 Million Text Messages
- Netflix: 70,017 Hours Watched
- Apps: 342,000 Apps Downloaded
- Instagram: 46,200 Posts Uploaded
- Snapchat: 1.8 Million Snaps Created
- Twitter: 452,000 Tweets Sent
- Amazon: $751,522 Spent Online
- Spotify: 50 Voice-First Devices Shipped
- LinkedIn: 120 New Accounts Created
- Tinder: 990,000 Swipes
- LinkedIn: 156 Million Emails Sent
- Google: 40,000 Hours Listened

Created By: @LoriLewis
@OfficiallyChadd
Internet (Security) Today

- A computer connected to the Internet is exposed to a likely cyberattack every 39 seconds (Univ of Maryland)
- 37% of UK businesses experience Cyber attack or security breaches at least once a month
- Predicted Global annual Cost of Cybercrime is USD 4.5T
- 78% of people claim to be aware of the risks of unknown links in emails. And yet they click anyway
- 91% of Hacks Started With a Phishing Email
- Expected Spent on Cybersecurity to be USD 1 Trillion in the next 5 years

And yet,

Only 29% of the companies surveyed have written down cybersecurity policy
PKI Through History

- Diffe-Hellman and RSA in 1976-78
- First Electronic Transaction Laws (Utah 1995)
- Indian IT Act of 2000
- Various Applications: eProcurement, MCA21, Income Tax and others: 2005 to 2009 and continuing
- UIDAI and Aadhar (2009-15)
- eSign 2015-16 and continuing
- Algorithms based on ECC
Is PKI one of those profound Technologies?

- VPNs connecting enterprise Networks
- SSLs for payment web pages through the world
- E-Passports enabled by PKI
- Payments across the world: SWIFT system
- Payments and settlement in India (Check Truncation System, RTGS, NEFT)
- Several G2G, G2B and G2C applications in India
## Survey on Obstacles to PKI Deployment and Usage

<table>
<thead>
<tr>
<th>Obstacle</th>
<th>Major Obstacle %</th>
<th>Minor Obstacle %</th>
<th>No Obstacle</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software Applications: Don’t support</td>
<td>54</td>
<td>33</td>
<td>10</td>
</tr>
<tr>
<td>Costs too high</td>
<td>53</td>
<td>34</td>
<td>12</td>
</tr>
<tr>
<td>Poorly understood</td>
<td>47</td>
<td>41</td>
<td>11</td>
</tr>
<tr>
<td>Poor Interoperability</td>
<td>46</td>
<td>39</td>
<td>12</td>
</tr>
<tr>
<td>Too Complex</td>
<td>46</td>
<td>39</td>
<td>13</td>
</tr>
<tr>
<td>Hard to Use</td>
<td>43</td>
<td>42</td>
<td>13</td>
</tr>
<tr>
<td>Too much legal work</td>
<td>25</td>
<td>50</td>
<td>22</td>
</tr>
<tr>
<td>Hard for IT to maintain</td>
<td>20</td>
<td>55</td>
<td>21</td>
</tr>
</tbody>
</table>
eSign

- eSign promises to be one of those profound technologies which work under the hood
- Based on Aadhar, almost ubiquitous in India
- Low cost of usage
- Easy to deploy
- Can be deployed with practically all online applications
Thank you