Unique Identification Authority of India (UIDAI)

Government of India (GoI) Bangla Sahib Road, Behind Kali Mandir, Gole Market

New Delhi - 110001

SECURE QR CODE SPECIFICATION

MARCH 2019

Table of Contents

1. Introduction

Secure QR Code currently presents on Aadhaar print-letter and e-Aadhaar. It contains only the demographic information of the Aadhaar holder. UIDAI is replacing the existing one with a new Secure QR Code which will now contain demographics as well as photograph of the Aadhaar holder. Information in Secure QR Code will be made secure and tamper-proof by signing it with UIDAI digital signature.

1.1 Target Audience

This is a technical document and is targeted at agencies who wanted to use the aadhaar secure QR code to validate the resident.

1.2 Legal Framework

The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act 2016 was published in gazette notification on March 26, 2016. The Act is to provide for, as a good governance, efficient, transparent, and targeted delivery of subsidies, benefits and services to Aadhaar Number holders. A gazette notification was issued by Central Government on 12th July 2016 to establish UIDAI as an Authority and operationalize certain provisions of Aadhaar Act 2016. Authentication regulations are also published under this Act. These documents specify legal framework for authentication usage, AUA/ASA engagements, audits, and other details. Detailed partner documents are also published. These documents are available at http://uidai.gov.in/.

1.3 Objective of this document

This document provides specification and logic for Secure QR Code. It contains details including data format, validation logic and specifications.

2. SECURE QR CODE

Secure QR Code can be scanned and resident details can be verified against provided Aadhaar / eaadhaar copy. Secure QR code contains demographics as well as photograph of the aadhaar holder. This information is signed so as to make it tamperproof.

2.1 Channels to avail service

Secure QR code is available in eaadhaar and Aadhaar print letter. In future this will be available in offline ekyc service also.

2.2 Data **fields**

Secure QR code is dividing into four parts.

- Text Data: Text data contains the following data fields in given sequence, which is embedded in byte array with the delimiter of byte value"255"
  a. Email_mobile_present_bit_indicator_value (can be 0 or 1 or 2 or 3): 0 : indicates no mobile/email present in secure qr code. 1: indicates only email present in secure qr code. 2: indicates only mobile present in secure qr code 3: indicates both mobile and email present in secure qr code.
  b. referenceId
  c. name
  d. date of birth
  e. gender
  f. care of
  g. district
  h. landmark
  i. house
  j. location
  k. pin code
  l. post office
  m. State
  n. Street
  o. Sub district
  p. VTC
- Photo of the resident: JP2000 Photo embedded in byte array after text data. No delimiter available for photo
- E-mail Id and Mobile number: Hash value of email and mobile is converted into byte (fixed size - 32 bytes each for email and mobile) embedded into the Secure QR code byte array.
- Signature: Signature value is embedded in Secure QR code byte array in the last. Size is fixed as 256 byte.

3. Specification

3.1 Data Format:

Sequence of embedded data in Secure QR Code:

- 0, 1, 2, 3: 0 - no mobile/email. 1- Only email. 2 - Only mobile. 3 - Both email/mobile
- referenceId – last 4 digits of Aadhaar code and date time stamp in "DDMMYYYYHHMMSSsss" (including milliseconds)
- name
- date of birth
- gender
- Address : care of
- Address : district
- Address : landmark
- Address : house
- Address : location
- Address : pin code
- Address : post office
- Address : State
- Address : Street
- Address : Sub district
- Address : VTC
- Photo of the resident (highly compressed including face only in JP2000 format)
- email as hash (hashing logic same as offline xml) [fixed size - 32 bytes]
- mobile as hash (hashing logic same as offline xml) [fixed size - 32 bytes]
- Signature HASH [fixed size - 256 bytes]

3.2 Validation steps:

- Convert the base10 value of Secure QR code into Big Integer.
- Convert the Big Integer into byte array.
- Decompress the byte array.
- Read the value of byte array from index 0 to till first delimiter value "255" and convert this byte array value into string with encoding "ISO-8859-1". We will get the Email_mobile_present_bit_indicator_value as 0, 1, 2 or 3.
- Read the value of byte array from next index (index will be last presence of delimiter value +1) till we hit the next delimiter value "255" and populate the appropriate field..

- Repeat step 5 till we get value of the VTC field.
- Now read the value of signature from end (Byte array length -1) till 256 byte in reverse order. Signature size is of fix length of 256.
- Post getting signature value, check the value of Email_mobile_present_bit_indicator_value:
    - if its 3 then first read mobile from index (Byte array length – 1-256) and then email from index (Byte array length – 1- 256- 32) in reverse order. Each value will be of fix size of 32 byte.
    - If Email_mobile_present_bit_indicator_value is 1 then only mobile is present.
    - If Email_mobile_present_bit_indicator_value is 2 then only email is present.
    - If Email_mobile_present_bit_indicator_value is 0 then no mobile or email present.
- Email and Mobile value will available in byte. Convert into Hexadecimal String.
- At last read the photo from index (VTC delimeter value of "255" + 1) to index (Byte array length – 1- 256 – (if mobile present then -32 if email present then -32))
- Remove the signature value from secure qr code byte array to get signed data.

- Now validate (signature value and signed data value) by using public key with algorithm SHA256withRSA.

- To verify mobile/email, first obtain the fourth digit of reference id (last digit of Aadhaar number). If it is 0 or 1 then converts provided Input mobile/mail id into sha256 value of provide data. In case of 2 to 9 convert the sha256 value for same number of times. This converted value should match with the value received in 8. If value not matching means mobile/email not verified.

Sample Data:

697941484820554848161929944287990190089397833259461440704476771748 5
407280104077714658698163325401659212830920734233047578454701810567 0
320152702236829179158252347037547125048879213091817896078091688845 8
384839645665300702247935633624019813036393088163236712473854151749 9
494458139647378808680614169273221404741476596583953169248831376224 3
963351695770648129871405781448858194791901735376449702321251422539 6
378497913801131879838544243609990162199828362481607008050483071259 4
525760596934341576755626791590403636878139861665599383319429228364 4
341839131979587386970014104938392812986923428299515667125303097587 5

936464970115363992197979842970756619926195003741817132928320737204801494866916066677619841404063338467710471769750752171758677670908420036495617886363610598886726092988757709295557040780378302139789734199991461679044102983722912974666922509563320109764432159350250340444071411051516703488912825896558343596503022584534856458205152134880074257444287708777419466898351662963107334120270545338278061377542733694928338808489165448422544694094166094244063778474429325991647984140708818946296448967023186648190423733849487281309889087584564003437037038710879895018022086543601275248721667704181731293011974760101780757756541397754569337548013132424069609987947943672257656644793959319559068459126180903802312217817200615049956918521883874933723828159703728892446400999753093833679817602359729232832096508699018453142618886296540831330897349592496514411339659382909064526665331377458203613898201336856147471915444713489446661156058975825182906322637030028217582347956984726143934840455825140227373086505348221458918002830204382143835758330281837414397399700274504752640575576040704500669442350133708178029981508032484033782881264430004190035681642911426109823019897675202600207987688279659723561501559448618205778147615291817074640315700521689623942852170603346606158760806503613315307443219595213136856423416800544777019034577702491762987963917116719929852078265309160759260989590618158889891835294735614366674503961584445497685736312628248483551986529867423016255476553691922054241686230968975229511700928171281549902682365302333677412951788839806869796040512235899311734337858684531156721416280114473368826463098485252394260075790386415875290922570568686439586036262465414002334117870088922801660529414759784318799843806130096998190881240404138869292933097823353052967206662202433041750863582782113557899579980148012093322934589404638591065919864345204338105835693092249292642282638414773789493293124439582159392944326694642602165340745608827230068384597928123402530783302911355269526752037908334302378528317406014331983642433635697302053510773934416911412400559008190912299316051468655201830018102397084643225883899560362917601755588438191054182345802396101743236366060952627229401437060636988464996732853776211805705377881603049368099152378894893423878910570127837266949201845732027896729639223800282711244480242656443966863415084478303513802421275423938494102838304095949885032467995444446876069548815105975156864109938289075889796991411801608930626033381048579032398458567831302759354135692754399087899833116632119374492594442598989727662 08

4. Appendix

4.1 References/Any additional info:
