Globally Identifiable Number (GIN) Registration

Adam Roach
`draft-ietf-martini-gin-05`
MARTINI / IETF 78
July 29th, 2010

Changes Since -03

- Terminology realignment (phone number ⇒ AOR, treminal ⇒ UA, PBX ⇒ SIP-PBX), editorial improvements.
- Clarified handling of feature tags, option tags in REGISTER
- Changed "user" parameter handling: now forbidden on "bnc" URIs; SSP follows 3261 rules to insert as appropriate.
- Clarified contents of "reg" event bodies.
- Added analysis of interaction with "outbound" mechanism.
- Added "Security Considerations" section.

Ticket #48: Requirements Analysis

- Editorial changes in REQ 4, 5, 10, 14, 15; the evaluation in GIN requires no change.

- Original REQ 17, DES 4 have been removed.

- Proposal: -06 to reflect new requirements language, with no change to evaluation text.

Ticket #49: Nits

- Agree with John on all points except placement of comma.
- Proposal: all other changes to be incorporated in -06.
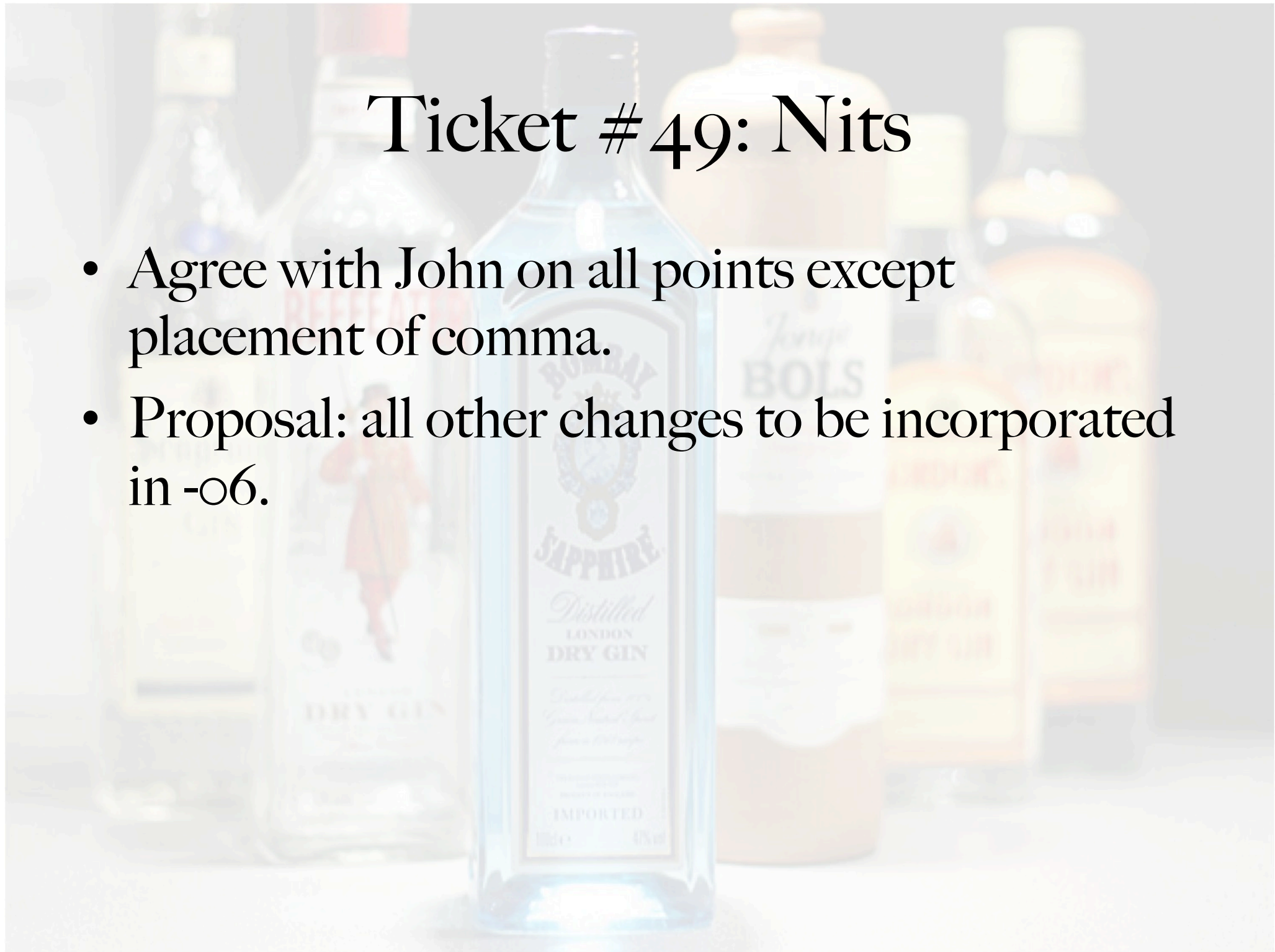
Ticket #50: Minor Issues

- Issues 1 – 3: propose updating -06 with John's suggestions
- Issue 4: Propose:
  - The SSP registrar then maps I_i to the ~~"bnc" AOR template~~ Contact and instance ID using the database...
- Issue 5: Propose:
  - It includes the form of the URI it expects to receive in the Request-URI in its "Contact" header field

Ticket 51: Mandate specific behavior for out-of-spec Contact URIs

- Currently, if a Contact URI arrives with both "bnc" and a user *portion* (or "bnc" and a user *parameter*), the spec gives the registrar the option to ignore the unexpected part, or to completely reject it.

- Proposal: Update to specify that incorrect URIs always cause rejection.

Ticket #54: Editorial

- Simple clean up, suggest accepting Hadiel's change:
  - When an incoming request arrives at the SSP for a GRUU corresponding to a bulk number contact ("bnc"), the SSP performs slightly different processing for the GRUU than ~~a Proxy/Registrar would~~ it would for a non-"bnc" URI.

Ticket #55: "bnc" and "reg" events

- Hadriel has some nondescript heartburn over statement that the "bnc" parameter can't appear in "reg" event bodies
- The logic behind the prohibition is based on the fact that subscribers won't generally have any clue what "bnc" means.
- Proposal:
  - In particular, the "bnc" parameter is forbidden from appearing in the body of a reg-event notify <u>unless the subscriber has indicated knowledge of the semantics of the "bnc" parameter. The means for indicating this support are out of scope of this document</u>.

Ticket #56: Security Review

- Proposal #1: Remove properties #2 and #3 from list of cookie properties; add "unforgeability" as a property.

- Proposal #2: Add text to security section warning about DoS attacks based on overwhelming SSP with RSA computations using bogus temp GRUUs. Can mitigate with rate-limits.

Ticket #57: GRUU Mandatory?

- Arguments for: without at least SSP support of GRUUs, SIP-PBXes are dead in the water regarding privacy.
- Arguments against: SSP might have alternate privacy mechanisms.
- Options:
  1. Completely optional
  2. Mandatory to implement, optional to use
  3. Mandatory to use mechanism at all
- Proposal: Option #2.

Temp GRUU Procedures

BACKUP SLIDES

Temp GRUU Encoding: RFC5627
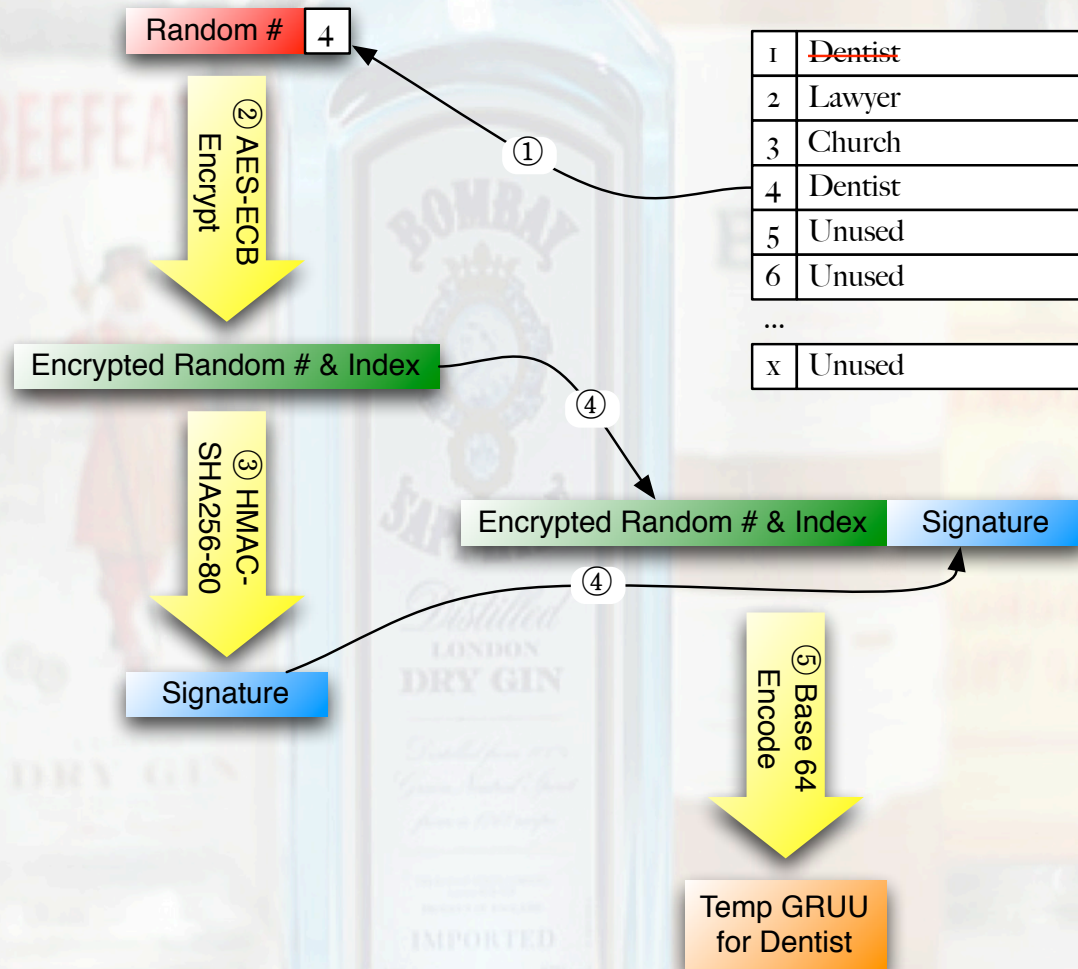
Temp GRUU Decoding: RFC5627

Temp GRUU for Dentist

① Base 64 Decode

Encrypted Random # & Index | Signature

② | ②

Encrypted Random # & Index | Signature

⑤ AES-ECB Decrypt | ③ HMAC-SHA256-80

④ Compare

Random # | 4 | Signature'

⑥

| 1	~~Dentist~~
2	Lawyer
3	Church
4	Dentist
5	Unused
6	Unused
...	
x	Unused
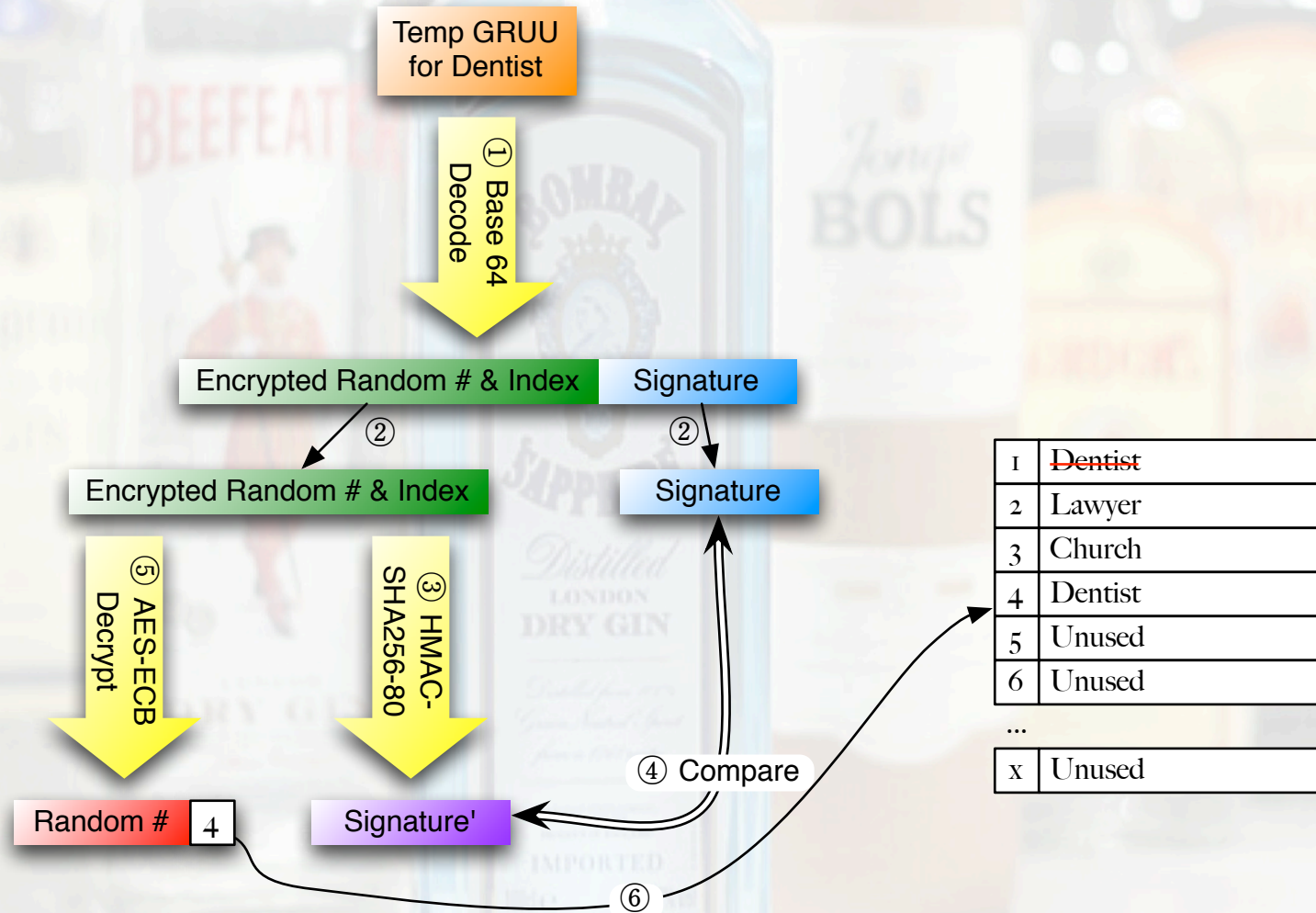
Temp GRUU Encoding: GIN
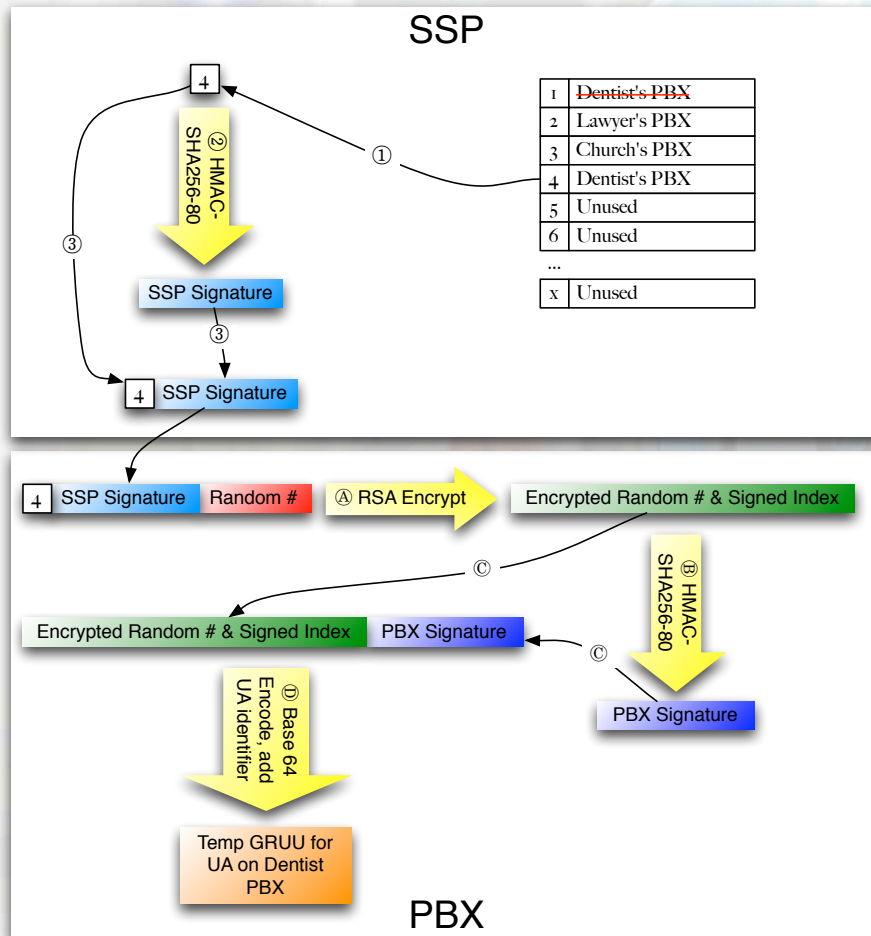
- Don't worry – this is drawn bigger on the next two slides

- In terms of crypto, only two differences from RFC 5627:
  – Includes additional signature on index
  – Uses RSA instead of AES-ECB

Temp GRUU Encoding: GIN SSP

Temp GRUU Encoding: GIN PBX

From SSP →

4 | SSP Signature

4 | SSP Signature | Random #

Ⓐ RSA Encrypt →

Encrypted Random # & Signed Index

Ⓒ

Ⓑ HMAC-SHA256-80

Encrypted Random # & Signed Index | PBX Signature

Ⓒ

PBX Signature

Ⓓ Base 64 Encode, add UA identifier
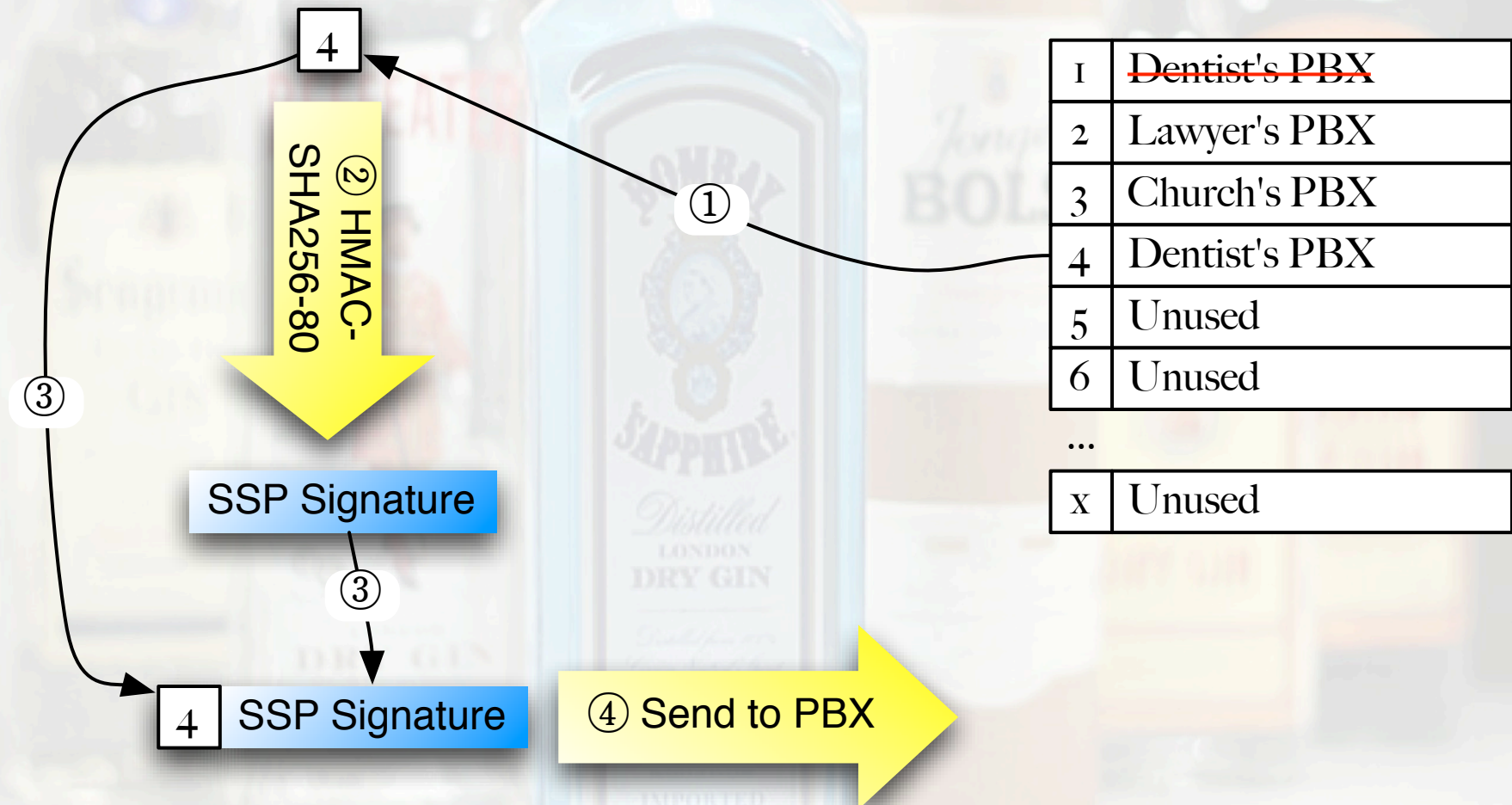
Temp GRUU for UA on Dentist PBX
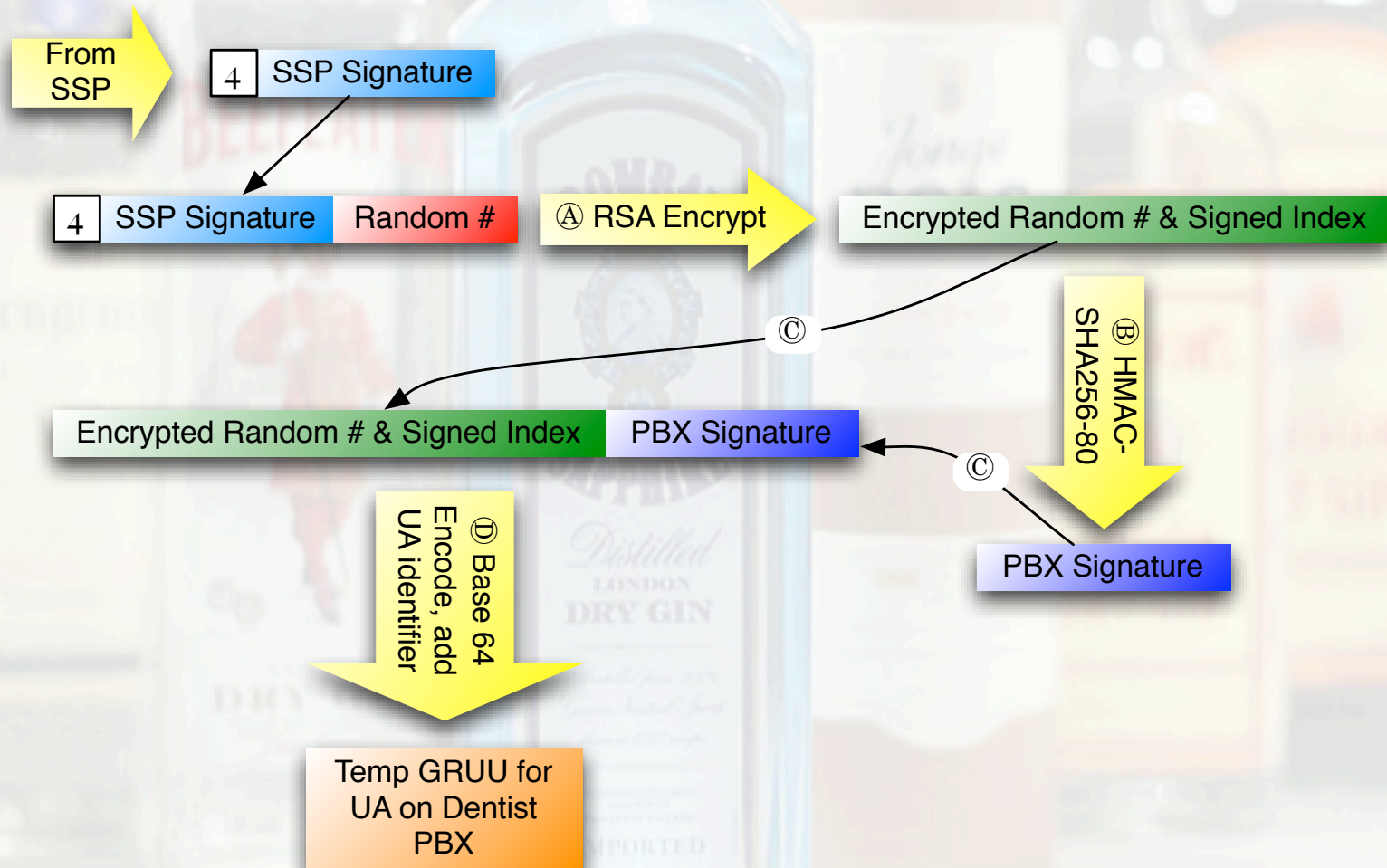
Temp GRUU Decoding: GIN SSP

Temp GRUU for UA on Dentist PBX

① Base 64 Decode, discard UA Identifier

Encrypted Random # & Signed Index | PBX Signature

②

Encrypted Random # & Signed Index

③ RSA Decrypt

④ HMAC-SHA256-80

1	~~Dentist's PBX~~
2	Lawyer's PBX
3	Church's PBX
4	Dentist's PBX
5	Unused
6	Unused
...	
x	Unused

4 | SSP Signature | Random # | SSP Signature'

⑤

SSP Signature

⑥ Compare

⑦

Temp GRUU Decoding: GIN PBX

Temp GRUU for UA on Dentist PBX

⑥ Extract UA Identifier

UA Identifier

① Base 64 Decode

Encrypted Random # & Signed Index | PBX Signature

②

②

Encrypted Random # & Signed Index | PBX Signature

④ HMAC-SHA256-80

PBX Signature' ⑤ Compare