

# BRSKI document status for IETF104, Prague. March 26, 2019

Authors:

Max Pritikin,  
Michael Richardson  
and  
Kent Watsen

# BRSKI document – passed WGLC

- Received Three reviews:
  - GenART review from Jari Arkko, see it here:
    - <https://www.ietf.org/mail-archive/web/anima/current/msg03866.html>
    - <https://mailarchive.ietf.org/arch/msg/anima/iVg7MRMdBQBVFA5VFiksYFHchBU>
  - SecDir review from Christian Huitema, see it here:
    - <https://mailarchive.ietf.org/arch/msg/anima/XCS6JpwQSm3naOivwCYaO0AAsVs>
  - IoT Directorate review from Russ Housley
    - <https://mailarchive.ietf.org/arch/msg/anima/1N7AR8hqu2oIWuTFFd9OQOab8S>
- Posted version -18 and -19 with incremental improvements, summary of final activities posted to mailing list
  - <https://mailarchive.ietf.org/arch/msg/anima/Sjr2Yy1YNfUw3WVv1EqOa7Swef0>

# Github Issues on BRSKI

- <https://github.com/anima-wg/anima-bootstrap/issues?utf8=%E2%9C%93&q=is%3Aissue+>
- Many improvements to text, added a number of sections:
  - (1) new section 5.3: Registrar Authorization of Pledge
  - (2) new section 3.1: Nonceless Voucher Requests
  - (3) new section 8: Applicability to the Autonomic Control Plane (plus other details in the document)
  - (4) new section 9: Privacy Considerations:
- Tried to narrow scope to ANI needs, lest ocean boiled.

Clear current search query, filters, and sorts

	0 Open	11 Closed	Author	Projects	Labels	Milestones	Assignee	Sort
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>					
add new section 1.3.x: Bootstrapping is not Booting. <a href="#">wglic-review</a> 2								
#114 by mcr was closed on 2 Nov 2018								
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>					
gen art issue #22: permanent vouchers... feature or bug. explain further <a href="#">email-reply</a> <a href="#">wglic-review</a> 2								
#110 by mcr was closed 14 days ago								
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>					
gen art issue #19: more requirements on MASA audit log <a href="#">wglic-review</a> 1								
#107 by mcr was closed on 13 Dec 2018								
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>					
gen art issue #7: serial-number in voucher issue <a href="#">wglic-review</a> 5								
#95 by mcr was closed on 17 Jan								
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>					
security review issue 11: what if MASA refuses to provide a voucher <a href="#">processed-posted</a> <a href="#">wglic-review</a> 6								
#88 by mcr was closed on 17 Jan								
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>					
security review issue 12: random number implementation <a href="#">wglic-review</a> 3								
#87 by mcr was closed on 2 Nov 2018								
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>					
security review issue 1: denial of service against vendor MASA service <a href="#">wglic-review</a> 4								
#81 by mcr was closed on 2 Nov 2018								
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>					
security review issue 2: compromise of vendor's public key <a href="#">email-reply</a> <a href="#">wglic-review</a> 5								
#80 by mcr was closed 14 days ago								
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>					
security review issue 6: ship and forget not supported <a href="#">email-reply</a> <a href="#">wglic-review</a> <a href="#">wontfix</a> 3								
#79 by mcr was closed 14 days ago								
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>					
security review issue 5: tampering during drop ship process <a href="#">wglic-review</a> 4								
#78 by mcr was closed on 5 Nov 2018								
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>					
security review issue 4: abuse of long duration infinite vouchers by a previous owner <a href="#">wglic-review</a> 3								
#77 by mcr was closed on 2 Nov 2018								

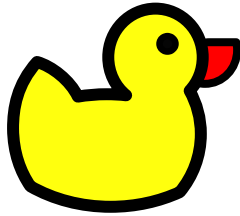
# Interop testing of BRSKI

BRSKI-19  
Contains many  
clarifications

- Being adopted by Thread Group
  - For details ask them.
- DOTS wants to use it
- Client (pledge) implementations from :
  - NXP, Silabs,
  - Signify, Cisco
  - Sandelman, Siemens (test client)
  - ZHAW
- In active Interoperability testing by FairHair Alliance
  - Third in-person session occurring Monday and Today.
- In use by [CIRALabs SecureHomeGateway](#)
- MASA / Registrar implementations from:
  - Siemens
  - [minerva.sandelman.ca](https://minerva.sandelman.ca)

# Some BRSKI iconology

- Pledge



Stajano, F. and Ross Anderson.  
"The resurrecting duckling: security issues for ad-hoc wireless networks", 1999.  
<https://www.cl.cam.ac.uk/~fms27/papers/1999-StajanoAnd-duckling.pdf>  
Wikipedia, "Wikipedia article: Imprinting", July 2015.  
[https://en.wikipedia.org/wiki/Imprinting\\_\(psychology\)](https://en.wikipedia.org/wiki/Imprinting_(psychology))  
[https://en.wikipedia.org/wiki/Animal\\_House](https://en.wikipedia.org/wiki/Animal_House)

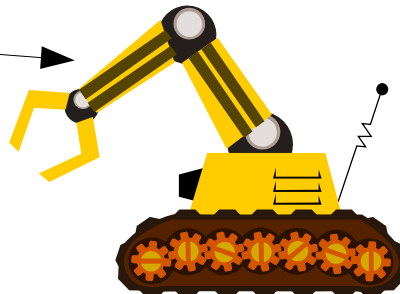
- Join Registrar/Coordinator



- JRC
- Registrar



- Manufacturer  
Authorized  
Signing  
Authority



-> MASA.



- VOUCHER
- RFC8366



# Major Issue for WG

- Should we completely remove unsigned pledge voucher request?
  - Offline case has **no** voucher request from pledge, and in the online case it seems to offer only illusion of security, with no significant reduction in crypto for pledge.
  - Was written as a compromise for limited devices, but constrained-voucher seems to be better fit.
- Corollary, should constrained-voucher include unsigned voucher requests? Always? Never?

# Document now with AD/IESG Questions?

?