Constrained voucher

draft-ietf-anima-constrained-voucher-14

Michael Richardson, Peter van der Stok, Panos Kampanakis, Esko Dijk

IETF 112
ANIMA Working Group
Constrained Voucher

BRSE Documents

- meta-info and html doc.
- BRSE Implementation
  BRSE comes in three components: pledge library, Registrar and MASA.

BRSE talks and tutorials
- Secure, zero-touch Bootstrap for the Internet of Things (IoTSF2018) (video)
- Prof. Andreas Rist on Authenticating Wireless Nodes in Building Automation: Challenges & Approaches
- Elot Lear on: Bootstrapping Remote Secure Key Infrastructures (BRSE) for Wi-Fi
- RIOT-OS 2019 talk about BRSE, Rust and RIOT-OS: Rusty Beer for RIOT-OS (PDF)
- Generic Animation of BRSE - Bootstrapping Remote Secure Key Infrastructure (OOP) (screencast)
- DINRG and ANIMA at IETF102
- NIST: Trusted IoT Network Device Project

EST: Enroute

BRSE: BRSE

SID: YARN

DSE: CBOR Signing and Encryption (RFC 8152)

MS: Cryptographic message Syntax (RFC 5652)

CBOR: Concise Binary Object Representation (RFC 7049)
Changes since IETF111

- Changes since version 13
- Clarify what the Updates are
- Much expanded BRISKI-EST section
- Some errors in SID allocation
- 17 issues open
  - (83 closed)
  - All review comments closed
- Security Considerations completed
- Added section on what to implement in specific Deployments
- Considered what to do if yang-cbor documents do not progress

---

**Table of Contents**

1. Introduction
2. Terminology
3. Requirements Language
4. Overview of Protocol
5. BRISKI-EST Protocol
6. Discovery, URIs and Content Formats
7. Extensions to BRISKI
8. Extensions to MASA
9. 6.2 VC-Discovery Protocol
10. 6.3.1 RFC9995 Telemetry Returns
11. BRISKI-MASA Protocol
12. PINNING Extensions to MASA
13. PINNING Extensions to EST-coaps
14. Artifacts
15. Voucher Request artifact
16. 8.1.1.1 Voucher Request artifact
17. 8.1.1.2 Voucher Request artifact
18. 8.1.1.3 Voucher Request artifact
19. 8.1.1.4 Voucher Request artifact
20. 8.2.1.1 Voucher Request artifact
21. 8.2.1.2 Voucher Request artifact
22. 8.2.1.3 Voucher Request artifact
23. 8.2.1.4 Voucher Request artifact
24. 8.2.2.1 Voucher Request artifact
25. 8.2.2.2 Voucher Request artifact
26. 8.2.2.3 Voucher Request artifact
27. 8.2.2.4 Voucher Request artifact
28. 9. Design Considerations
29. 10. Raw Public Key Use Considerations
30. 10.1. The Registrar Trust Anchor
31. 10.2. The Voucher Request
32. 10.3. The Voucher Response
33. 11. Security Considerations
34. 11.1. Clock Synchronization
35. 11.2. Protect Voucher PKI in HSM
36. 11.3. Test Domain Certificate Validity when Signing
37. 12. IANA Considerations
38. 12.1. Resource Type Registry
39. 12.2. The IETF XML Registry
40. 12.3. The YANG Module Names Registry
41. 12.4. The RFC SID range assignment sub-registry
42. 12.5. Media Types Registry
43. 12.6. CoAP Content-Format Registry
44. 13. Acknowledgements
45. 14. Changes
46. 15. References
47. 15.1. Normative References
48. 15.2. Informative References
49. Appendix A. Library support for BRISKI
50. A.1. OpenSSL
51. A.2. mbedTLS
52. A.3. wolfSSL
53. Appendix B. Constrained BRISKI-EST messages
54. B.1. Pledge Message
55. B.2. Registrar Message
56. B.3. MASA Message
57. Appendix C. Examples
58. C.1. Pledge, Registrar and MASA keys
59. C.1.1. Pledge private key
60. C.1.2. Registrar private key
61. C.1.3. MASA private key
62. C.2. Pledge, Registrar and MASA certificate
63. C.2.1. Pledge Certificate
64. C.2.2. Registrar Certificate
65. C.2.3. MASA Certificate
66. C.3. COSE signed voucher request from Pledge to Registrar
67. C.4. COSE signed voucher request from Registrar to MASA
68. C.5. COSE signed voucher from MASA to Pledge via Registrar
69. Authors' Addresses
70. ANIMA, IETF111, virtual
71. July 2021
Dependent upon CORE WG drafts - still in IESG review

yang-cbor/yang-sid design team formed to deal with review comments has had four meetings
• 18 issues still open (including a bunch of wontfix)
• 34 issues closed
• Design team includes Andy Bierman

My recommendation to ANIMA constrained-voucher team is that the SID documents will get through IESG review before Xmas break
Hackathon Results

- IETF112 Hackathon Nov 1-5. Meet up in gather.town @ 14:00 UTC, at table A(NIMA).
- Not really any participants. I think people (me included!) are exhausted.
  - BUT: L2 VPN now working, and we will test asynchronously.
- NIST NCCoE IoT-onboarding
Discussion

Thanks to weekly discussions in BRSKI design team on Thursday
Next meeting Nov. 25
Conclusions

Three directorate reviews occurred and were reacted to. Security Considerations is done. Applicability Statement is done.

Ready for WGLC!
• no major issues
• Only minor issues remain, many of which are wishes