A Comparison of CABF BR 1.1.6 and NIST IR 7924 DRAFT

CAB Forum Face to Face Meeting
Ankara Turkey
September 25-26 2013

Tom Albertson, Microsoft Corporation

AGENDA

Brief Overview of BR and IR

Observations

Conclusions & Recommendations

Suggested Timetable

Brief Overview of BR and IR

Purpose

BR

- Enable efficient and secure communications
- Address trustworthiness of certs

IR

- Baseline set of security controls
- Reference CP (IETF RFC 3647)
- US Govt Federal PKI (FPKI) as base document

Brief Overview of BR and IR

Notes on my review "methodology"

1. non-scientific, non-exhaustive: practitioner not a PKI expert
2. Comparison from the perspective of the BR, not the IR (Q: "does this BR section have an equivalent in the IR")

- Loses some valuable insights into actual scope of the IR, because lots of areas covered in IR that BR does not

3. May not be exhaustive (proponents should find fault with my review)

- Don't Worry: if we agree we can redo the review at the next draft IR and correct it

4. Reviewed DRAFT NIST IR versus BR v1.1.6 (July 2013)

- Final draft of NIST IR due out soon (November 2013)

5. I didn't review the Network System and Security Guidelines, EV Guidelines, or EV Code Signing Guidelines

Observations

Apples and Oranges

BR	IR
Loosely based on CP Format (but not RFC 3647)	Based on CP Format (RFC 3647)
Mix of CA specific items of primary concern e.g. Cert contents / profiles	Reference CP (template) - guidance, suggested text, fill in fields, instructions
Strength: Dynamic, prescriptive document	Strength: Solid presentation of all aspects of a proper CP, including guidance and suggested text
Strength: identity checking specifics, cert profile specifics	Strength: CA network and operational security specifics
Weakness: Inconsistent with RFC 3647 and terminology	Weakness: Lacks some of the international context of the BR

Observations

Overall, who do I think does better at:

BR Sections	CABF BR	NIST IR
Sections 1-8	Push	Push
Section 9 Cert Content and Profile	X	
Section 10 Cert Application	X	
Section 11 Verification Practices	X	
Section 12-13 Issuance / Revocation	Push/X	Push
Section 14-17 Employees, Data, Security		XXX
Section 18 Audit, Liability and Indemnification	XX	

Observations

We (CABF) can appreciate diversity of viewpoints
- e.g. WebTrust and ETSI audit regimes

We lead in important areas, but lag in others (security and terminology)

We operate in a PKI world that is converging on important aspects of PKI operations and security
- CABF BR, NIST IR, EC regulations?, ISO?

We want to reduce cost and complexity for all CAs and audit regimes
- We should adopt the CP structure and format of RFC 3647 now
- We should consider adopting the good guidance from NIST IR in areas that we lack, e.g. network and operational security guidance

We should optionally seek more formal participation in future NIST IR discussions and drafts

- Less scattering of complexity and more communication about key areas to both audiences, CABF and NIST.

Conclusions

NIST IR benefits from adherence to CP RFC 3647
- Design and focus is rooted in a single government PKI, but not irrevocably
IR document structure and terminology is more forward looking that CABF BR (other parties can read and comprehend)
Instead of positioning BR vs. IR (differences), both documents can look to CP RFC 3647
- With every ballot that adds non-RFC compliant terminology, we drive the BR further from the mainstream of PKI

Conclusions

CABF BR shines as a CA-centric, dynamic document to address baseline requirements

NIST IR's value is as a solid reflection on building CPs for publicly facing CAs

- guidance

CABF can quickly address immediate and specific needs on short cycles that benefit public CAs in terms of adoption

- BR – audit criteria – CA adoption

CABF doesn't benefit from divergence from RFC 3647 format or terminology, and will increasingly scatter the CA landscape

- All CAs benefit from one structure, which is RFC 3647

It is work that is better be done now, rather than later

Recommendations

Form a CABF WG to

1. Formally verify BR vs. IR comparisons (e.g. versus NIST revised IR)
2. Revise BR in compliance with RFC 3647 (reordering sections and content, not excluding BR content)
3. Adopt terminology to address differences
   e.g. Subscriber versus Applicant, TAMs versus Application Software Provider
4. Maintain Apples and Oranges Paradigm
   e.g. BR differs from IR in specifics but not in the particulars
5. There are some things in the BR that are just done in the PKI context we operate in.

Suggested Timeline

September 2013 – F2F Ankara: Form BR Revision WG

November 2013 (tentative) – NIST publishes revised IR 7924

December-February 2014 – WG reviews revised NIST IR 7924 and drafts new BR in RFC 3647 format and terminology

- Considers revised NIST IR content to fill in gaps in BR

February 2014 – F2F: preliminary presentation of WG work product at next F2F meeting

June – July 2014 – F2F: final draft presentation of WG work product

June-August 2014 - Ratification and Verification (auditability begins as early in WG effort as possible)

September 2014 – F2F: New BR presented for formal acceptance in annual revision timeframe (BR v2.0)