Blind RSA Signatures
draft-irtf-cfrg-blind-rsa
**Blind RSA Protocol**

Client:
- $\text{blind}_\text{msg}, \text{inv} = \text{Blind}(pk_s, \text{msg})$
- $\text{sig} = \text{Finalize}(pk_s, \text{msg}, \text{blind}_\text{sig}, \text{inv})$

Server $(sk_s, pk_s)$:
- $\text{blind}_\text{sig} = \text{BlindSign}(sk_s, \text{blind}_\text{msg})$
Draft Status

Updates and implementations

Draft updates:

• Add deterministic signature recommendation, test vector, and API considerations
• Improve security consideration
• Editorial cleanup

More interoperable implementations added
Questions

Closing remaining issues

Open questions:

• Should we consider changing the name? #1
• Should the draft support partially blind signatures? #29
• Should the draft add other blind signature schemes? #83
Questions
Closing remaining issues

Open questions:

• Should we consider changing the name? #1
• Should the draft support partially blind signatures? #29
• Should the draft add other blind signature schemes? #83

Proposal: **close all issues as WONTFIX**
Ready for RGLC?