The REGRR protocol

Daniel Kalchev, Register.BG

Protocol design

- Signed XML messages over encrypted communication channel
- No need to keeping session or state at the server
- Each message carries full authentication and authorization properties by virtue of digital signatures
- Regular command:object structure
- Nested message structure
- Nomenclature versions are communicated with each message
- The various nomenclature lists can be communicated between server and client

What REGRR achieves

- Secure communication with Registrars
- Secure communication with Registrants
- End to end encryption and signing
- Separate authorization of the Registrant and Registrar to modify Registry data
- Follows contractual relationships
- Solves the issues of Registrars having too much control over Registrant data

How it works

- The Registrant prepares and signs the message, possibly via the Registrar interface (could be web based or other protocol)
- The Registrar signs the Registrant message and communicates it to the Registry
- The Registry authenticates sources based on digital certificates and authorizes object modification based on object ownership and assigned rights
- The Registrant could authorize the Registrar to submit messages on their behalf
- The Registrant can communicate messages directly with the Registry, providing for secure updates for DNS and DNSSEC data.

Current implementations

- Implemented and published 2011 by Register.BG
- Three of .BG’s Registrars at various implementation levels
- Current server implementation runs on TLS/TCP
- Specification/documentation being translated to English…

Thank You

Daniel Kalchev, Register.BG
daniel@digsys.bg