

Authentication Update

ARIN DBWG

Tim Christensen

Overview

- * Mandate for change
- * Applying authentication to processes
- * Choosing the first method
- * Make it happen
- * Next steps

Why Change, Why Now?

- * Community has made it clear that mail-from authentication is inadequate and want better options
- * Stewardship principles dictate that ARIN move away from loose security
- * Release of new database clears path for forward progress

Applying Better Authentication

Identify use cases for authentication mechanisms: What processes benefit from stronger authentication?

- ▶ Inbound templates and requests
- ▶ Outbound mail
- ▶ Outbound files
- ▶ Web publishing
- ▶ Web transactions

Approach

- * Community has asked for spectrum of authentication choices
 - ▶ Password (md5-pw, des, etc.)
 - ▶ PGP
 - ▶ X.509
- * Implement one at a time, evaluate, and repeat
- * Consider mail-from deprecation after evaluating adoption progress

Authentication Deployment Precepts

- * Phased, opt-in adoption
- * Permit multiple authentication methods
- * Prohibit a POC's use of mail-from when an "improved" authentication method is selected by a POC

Choosing the First Authentication Method

- * Investigate other RIRs' implementations
 - ▶ APNIC – using userid/password, PGP, and X.509; running Certificate Authority (CA)
 - ▶ LACNIC – using userid/passphrase
 - ▶ RIPE NCC – using password and PGP

Choosing the First Authentication Method

* Community input – public policy mtgs.

- ▶ Certificates “good”
- ▶ When implementing PGP don’t use public key servers

* Engineering evaluation

- ▶ Applicability to processes
- ▶ Strength of security
- ▶ Coordination with other ongoing eng efforts
- ▶ Other RIR implementations

The choice: X.509 First

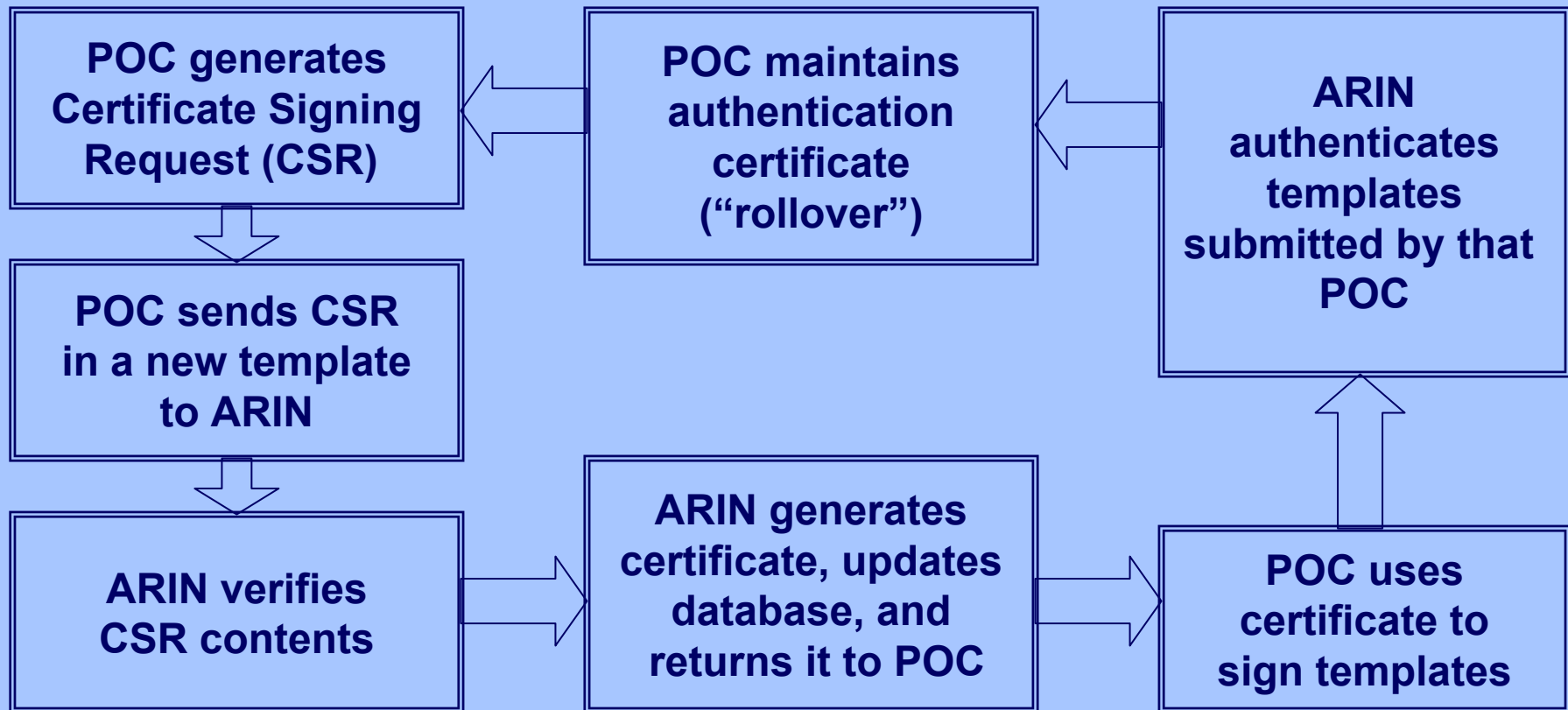
* Permits application of secure authentication to widest array of processes:

- ▶ Can protect (authenticate and encrypt) email templates
- ▶ Can authenticate web transactions
- ▶ Can authenticate data produced by ARIN

* Provides best combination of:

- ▶ Control
- ▶ Security
- ▶ Utility

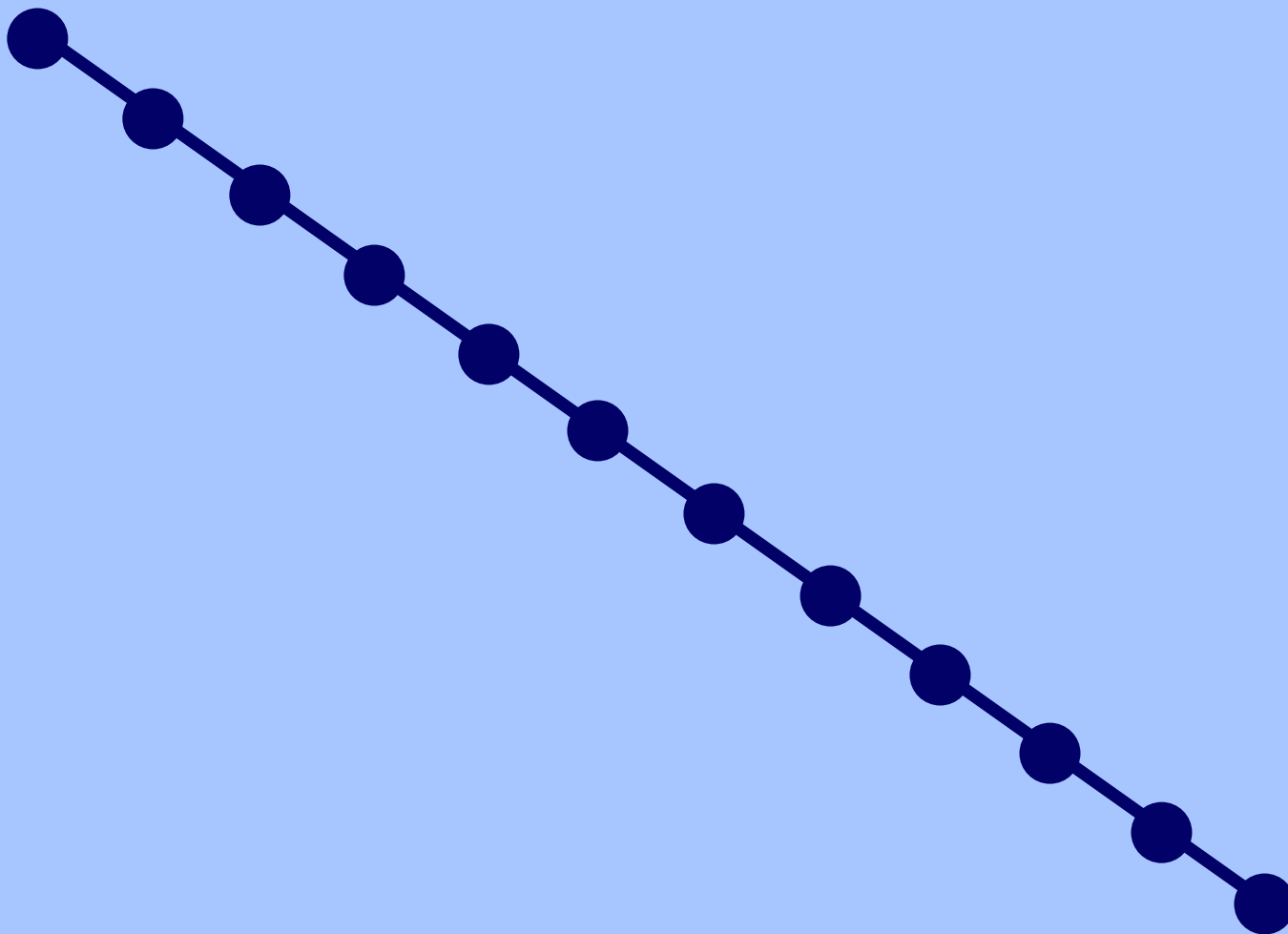
How X.509 Adopters Get Tighter Authentication



Getting There

- * Identify process touch points
 - ▶ Registration template processing (email)
 - ▶ Non-template email communication
 - ▶ Online processing (future)
- * Establish test bed
- * Propose process changes
 - ▶ CSR processing
 - ▶ Running the ARIN Certificate Authority (CA)
 - ▶ Signed template acceptance & rejection
 - ▶ Response to authentication failure

Timeline

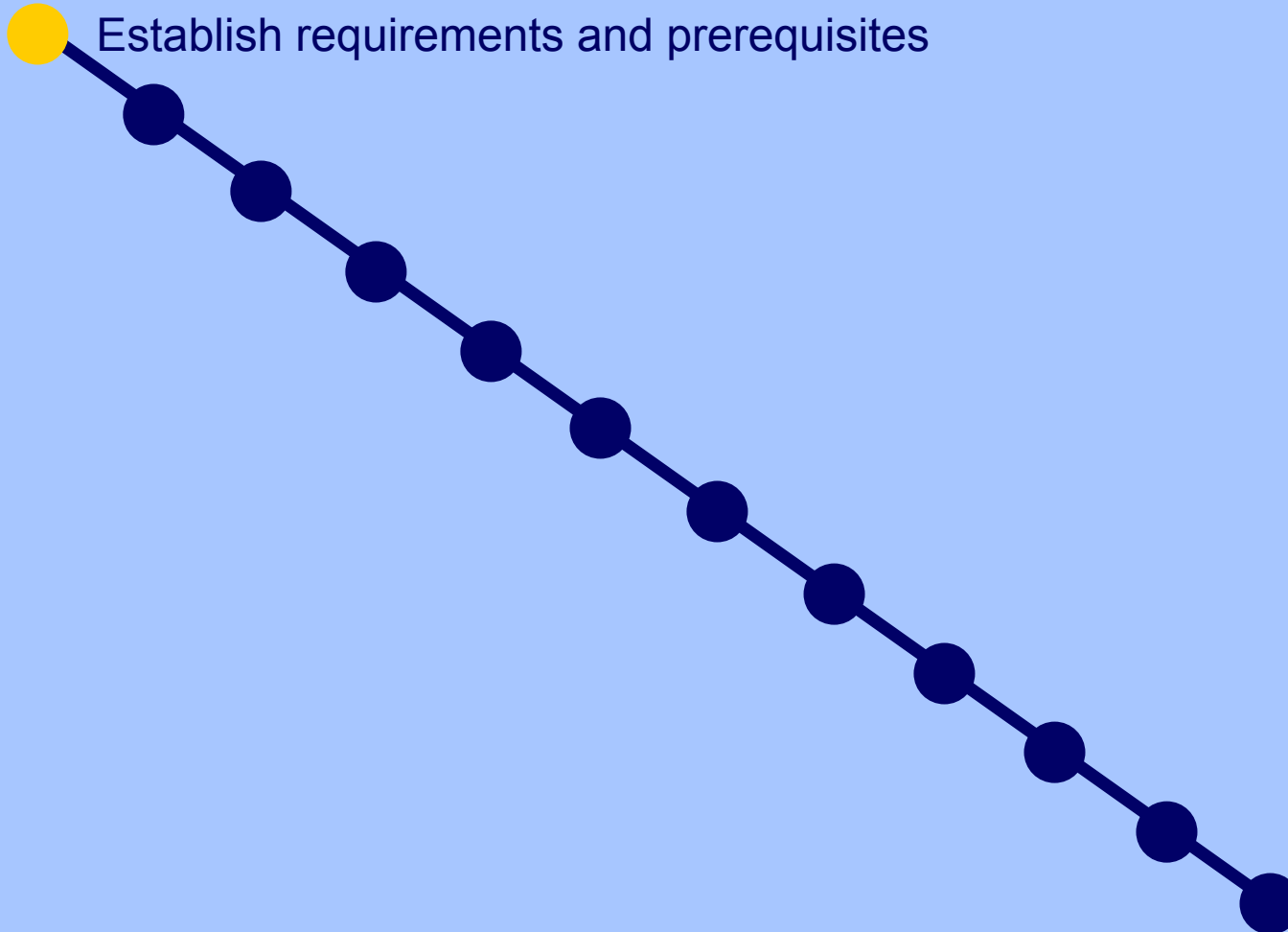


ARIN XI

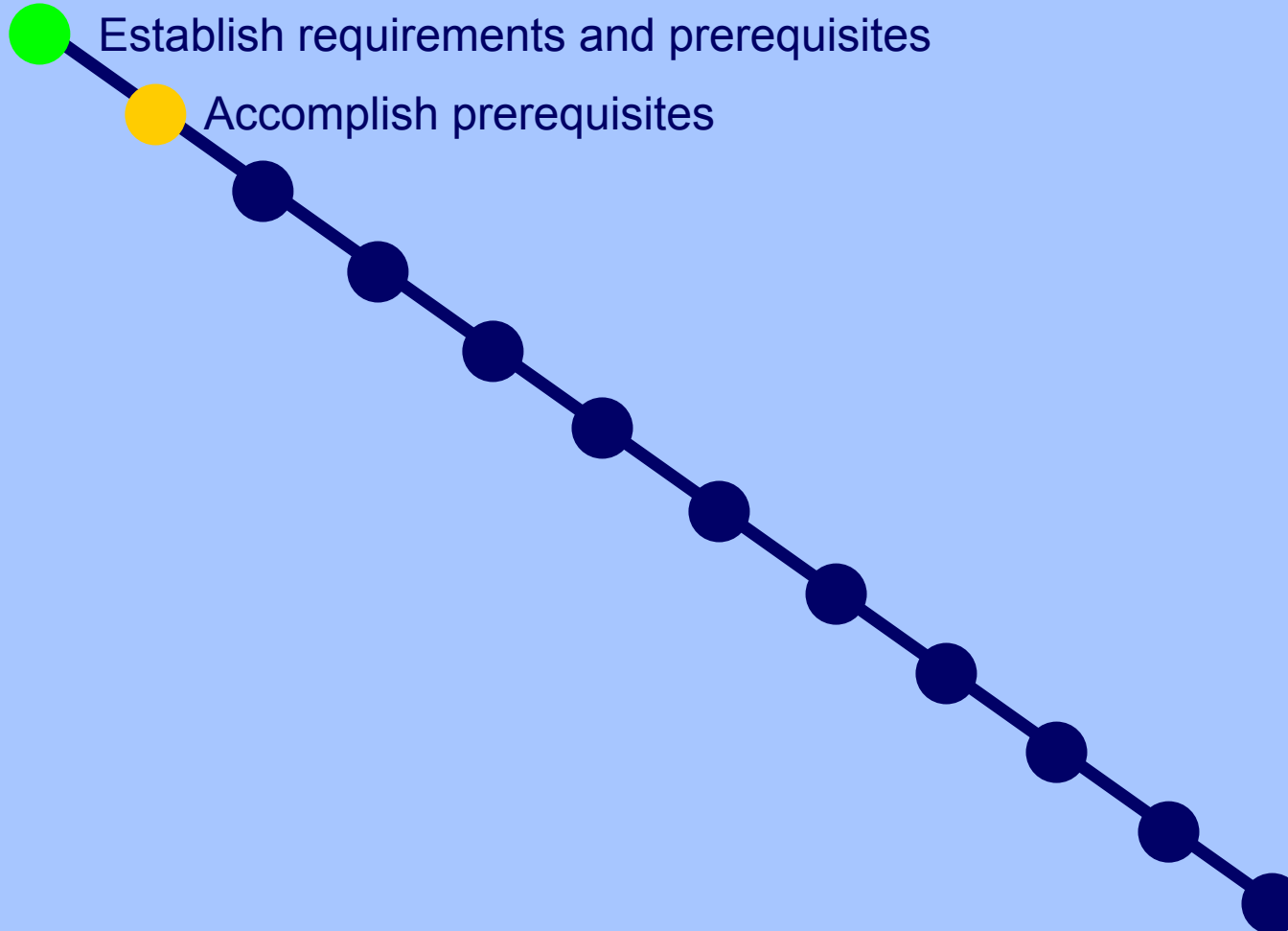
April 2003

Memphis, TN

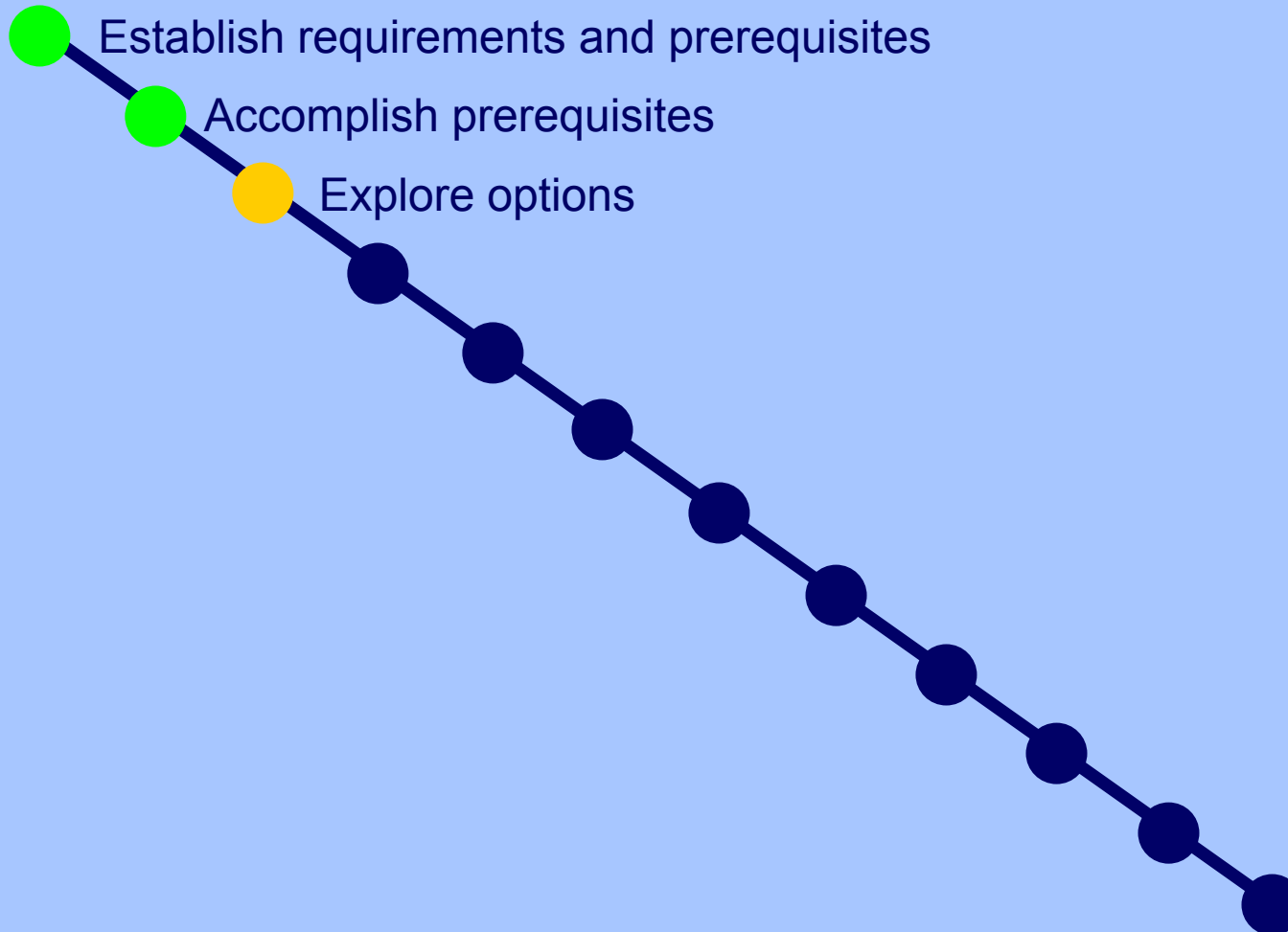
Timeline



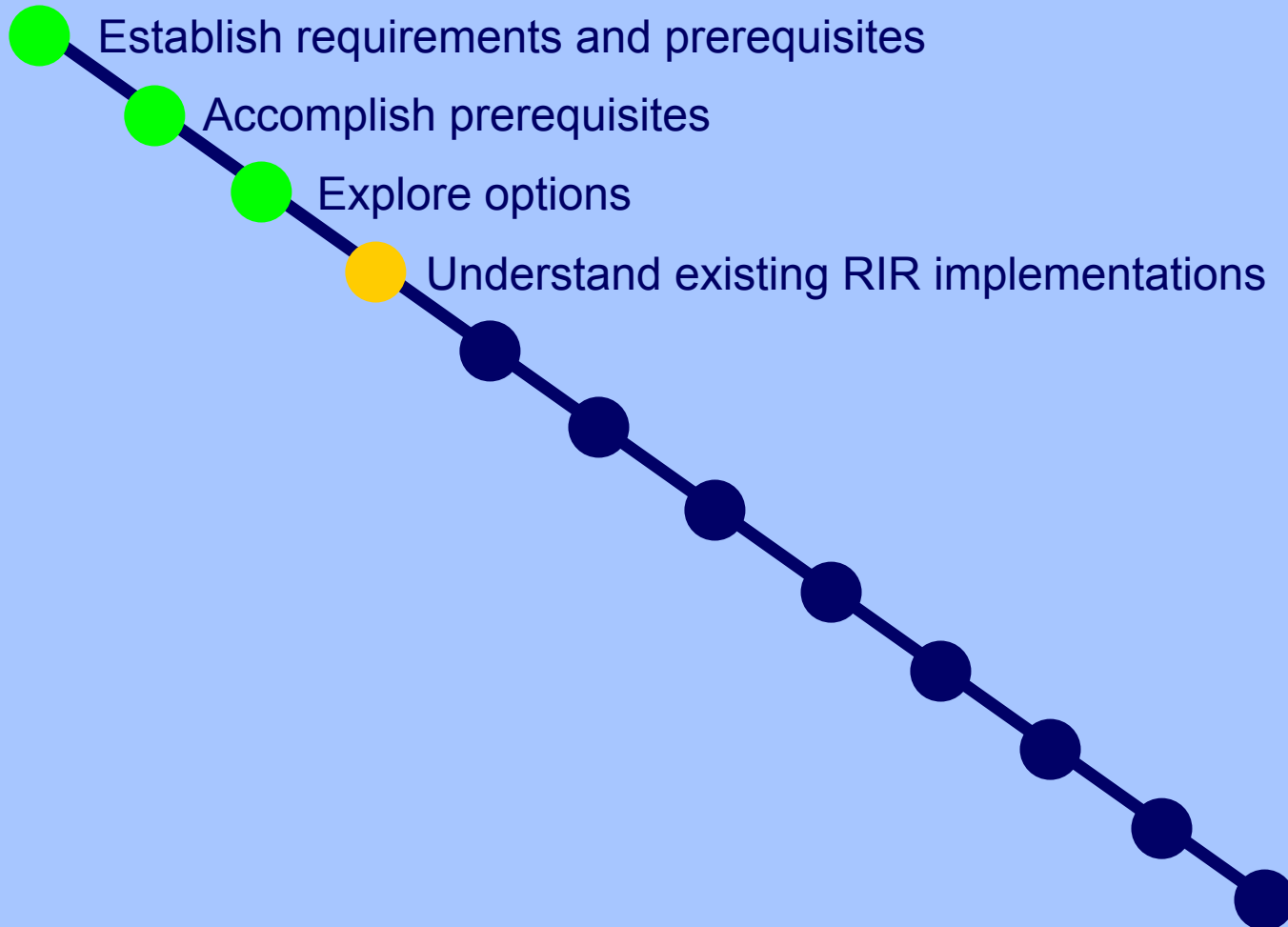
Timeline



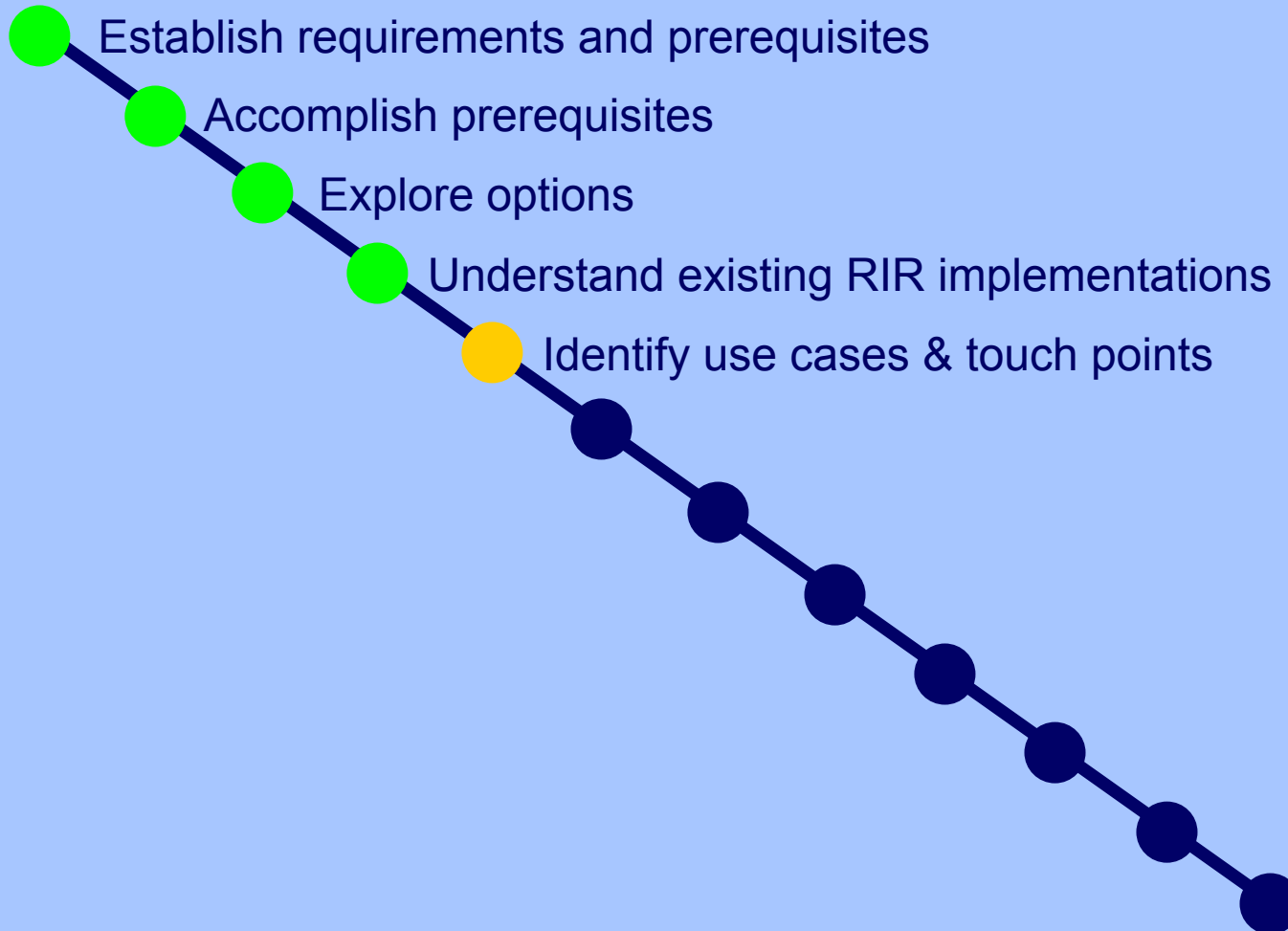
Timeline



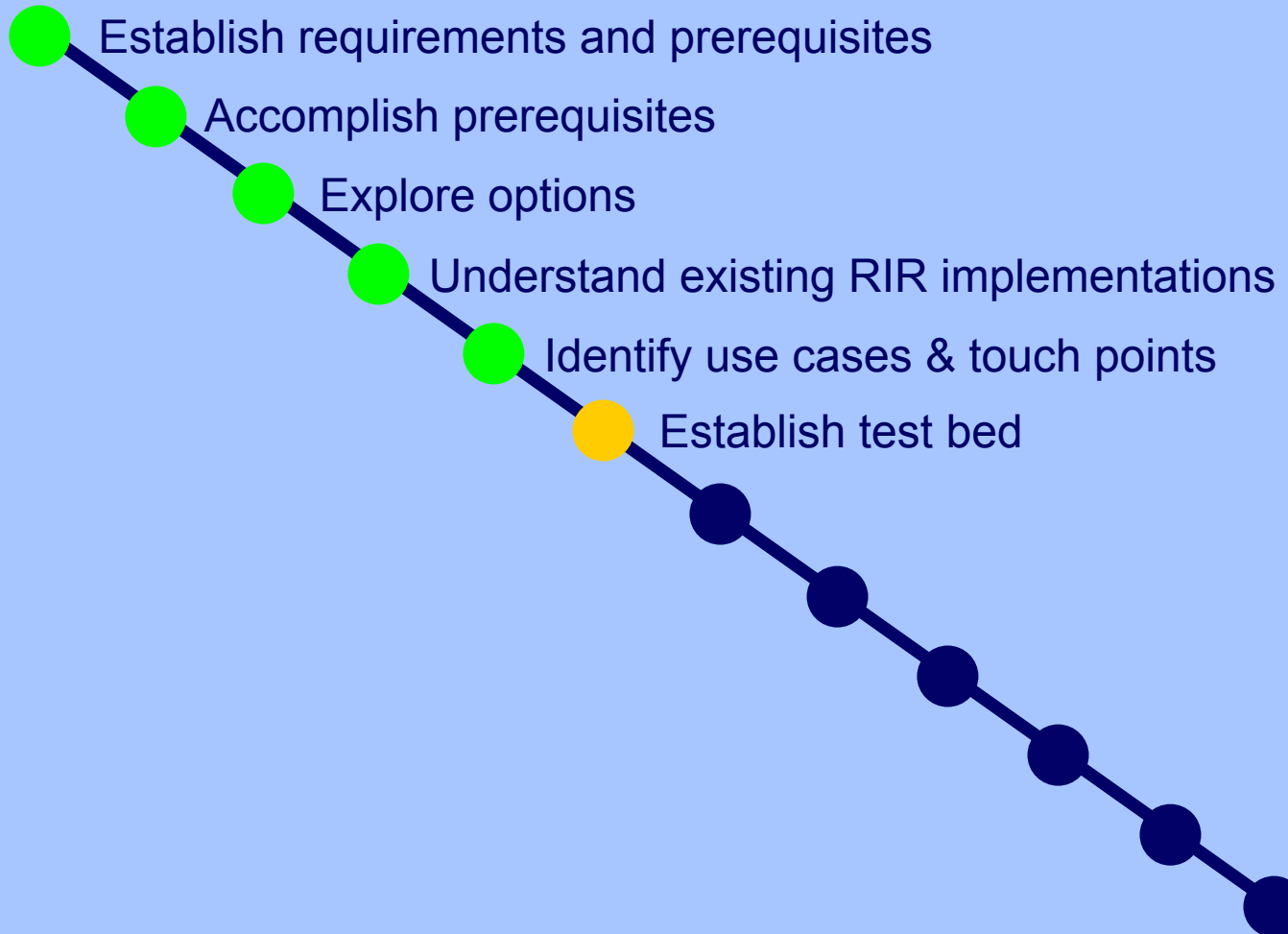
Timeline



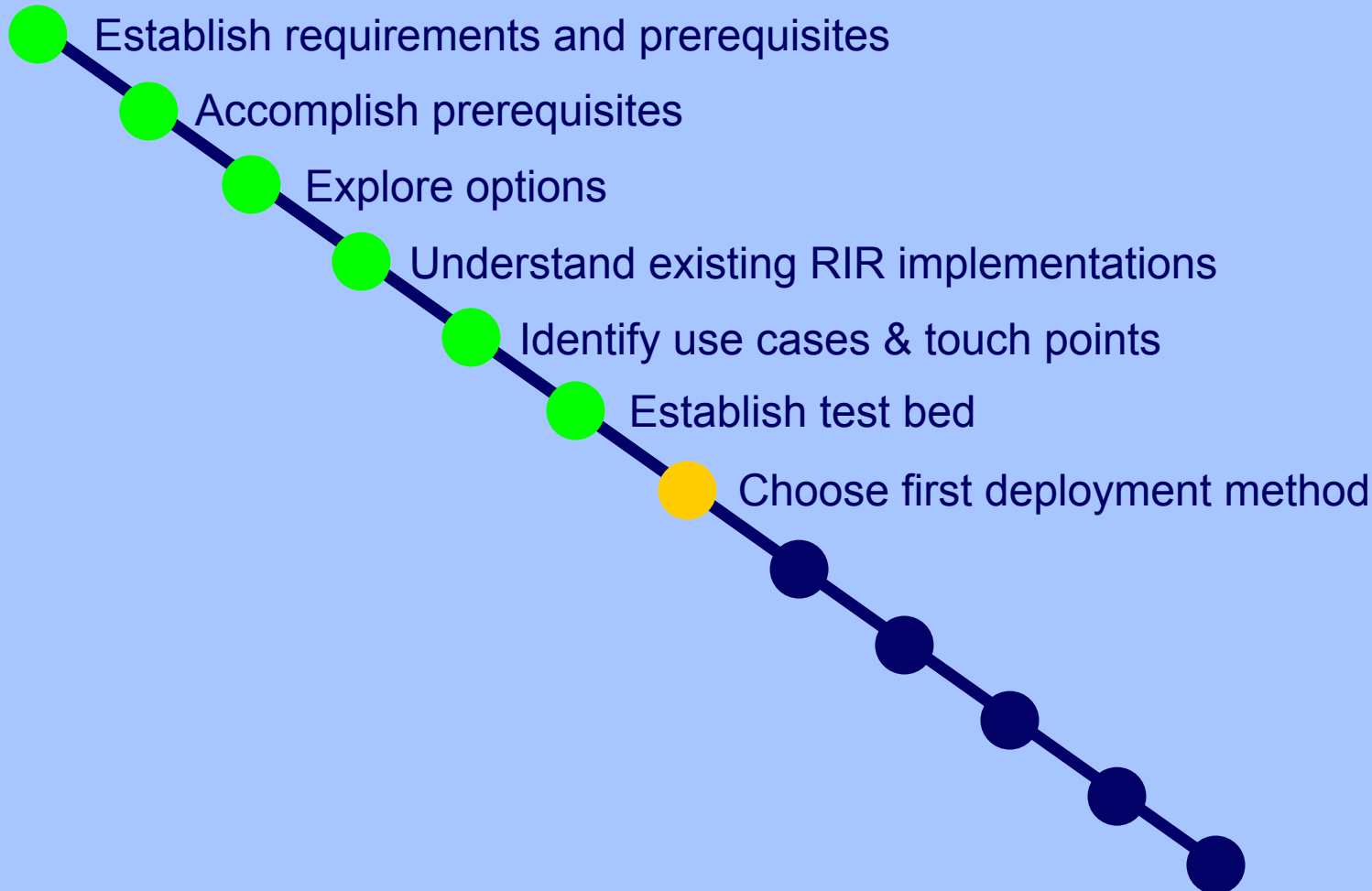
Timeline



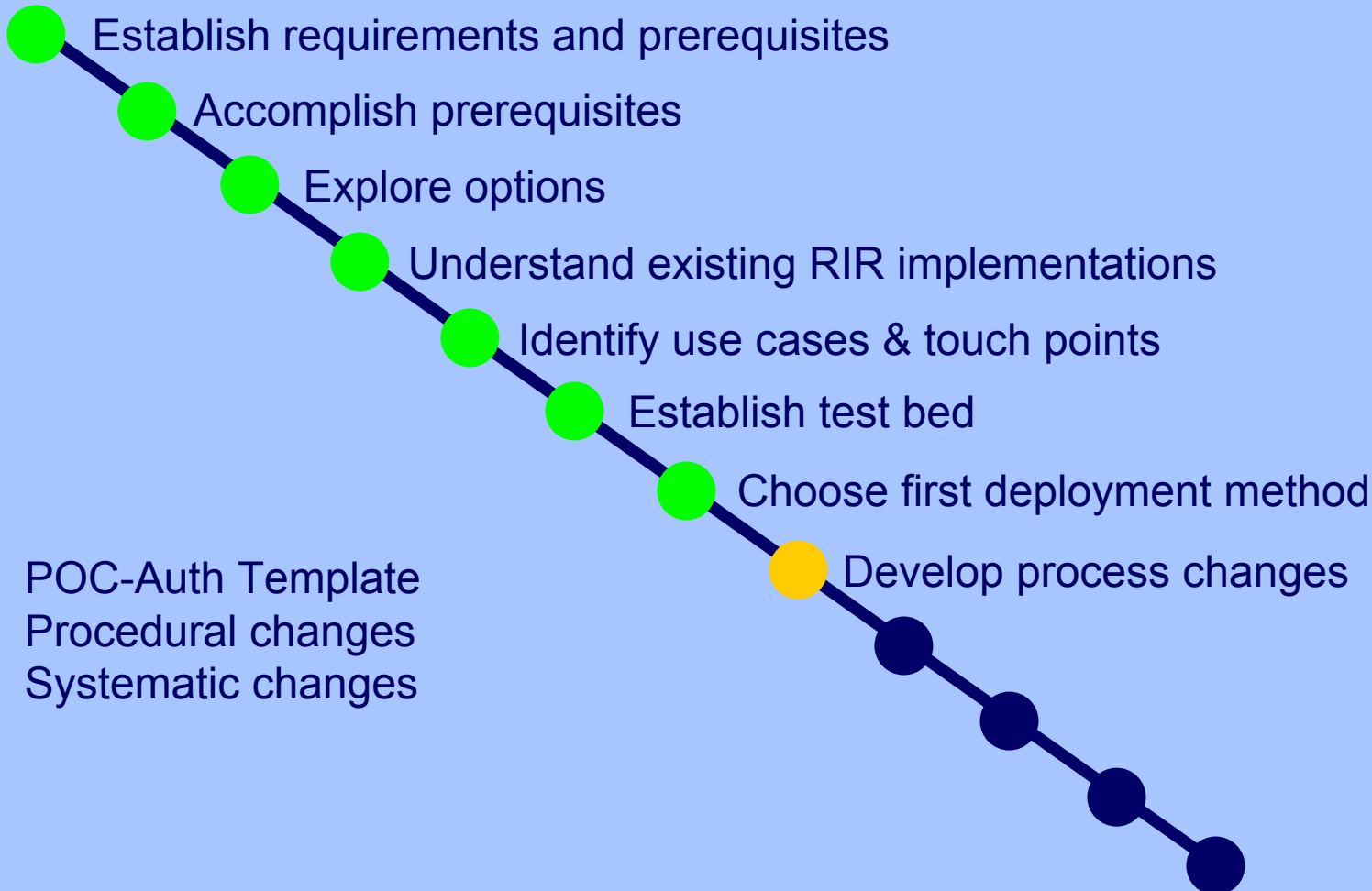
Timeline



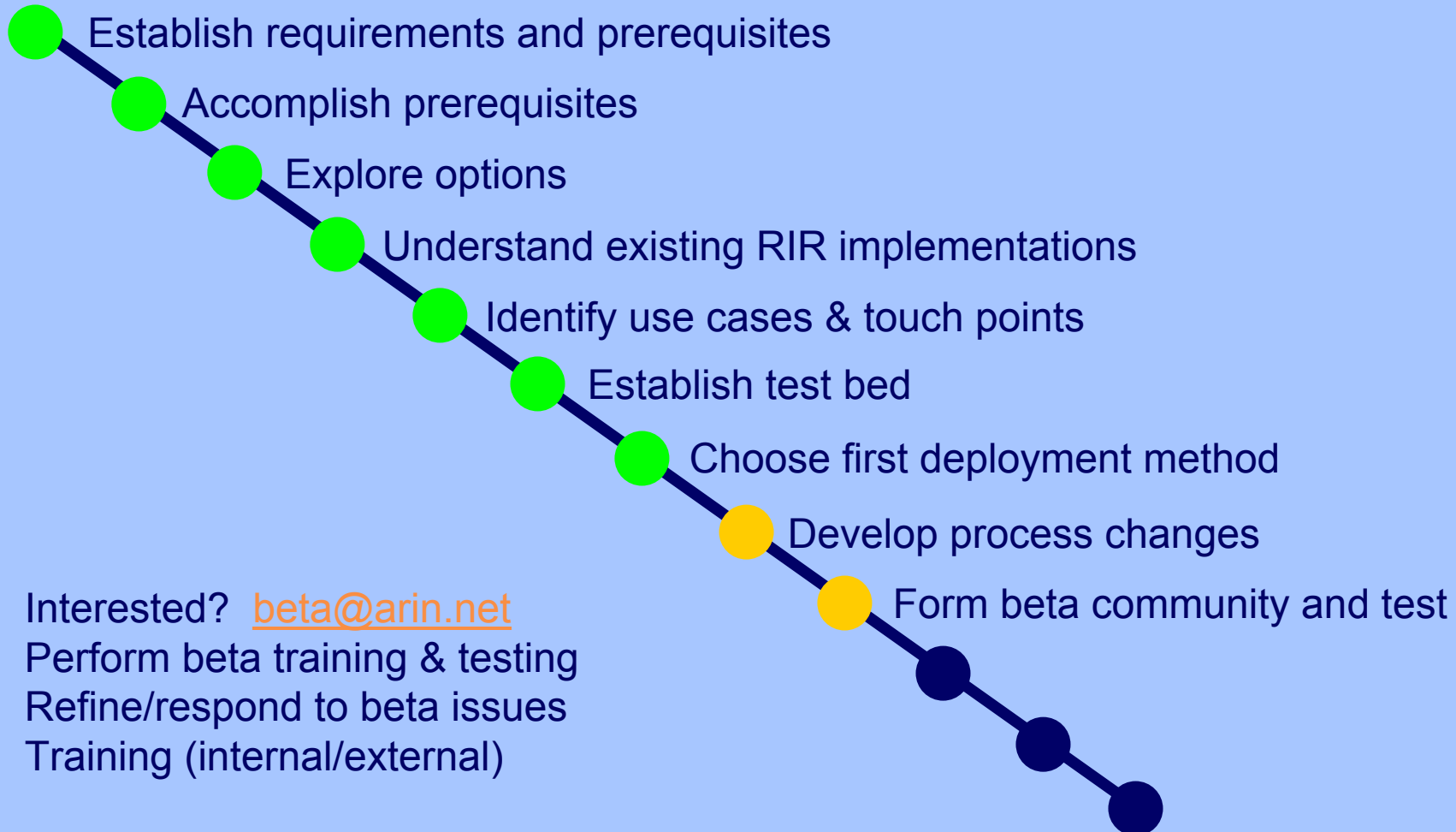
Timeline



Timeline



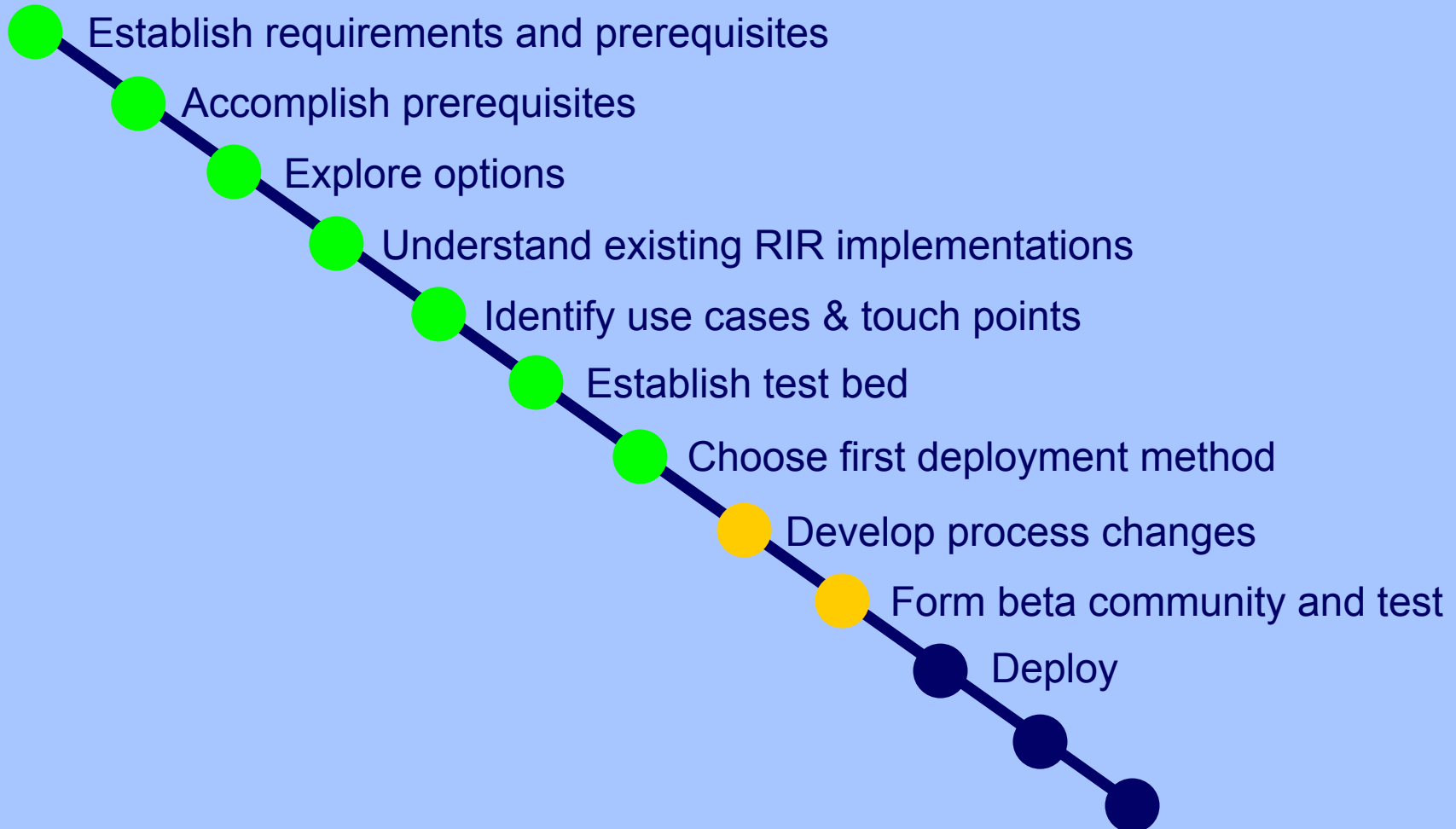
Timeline



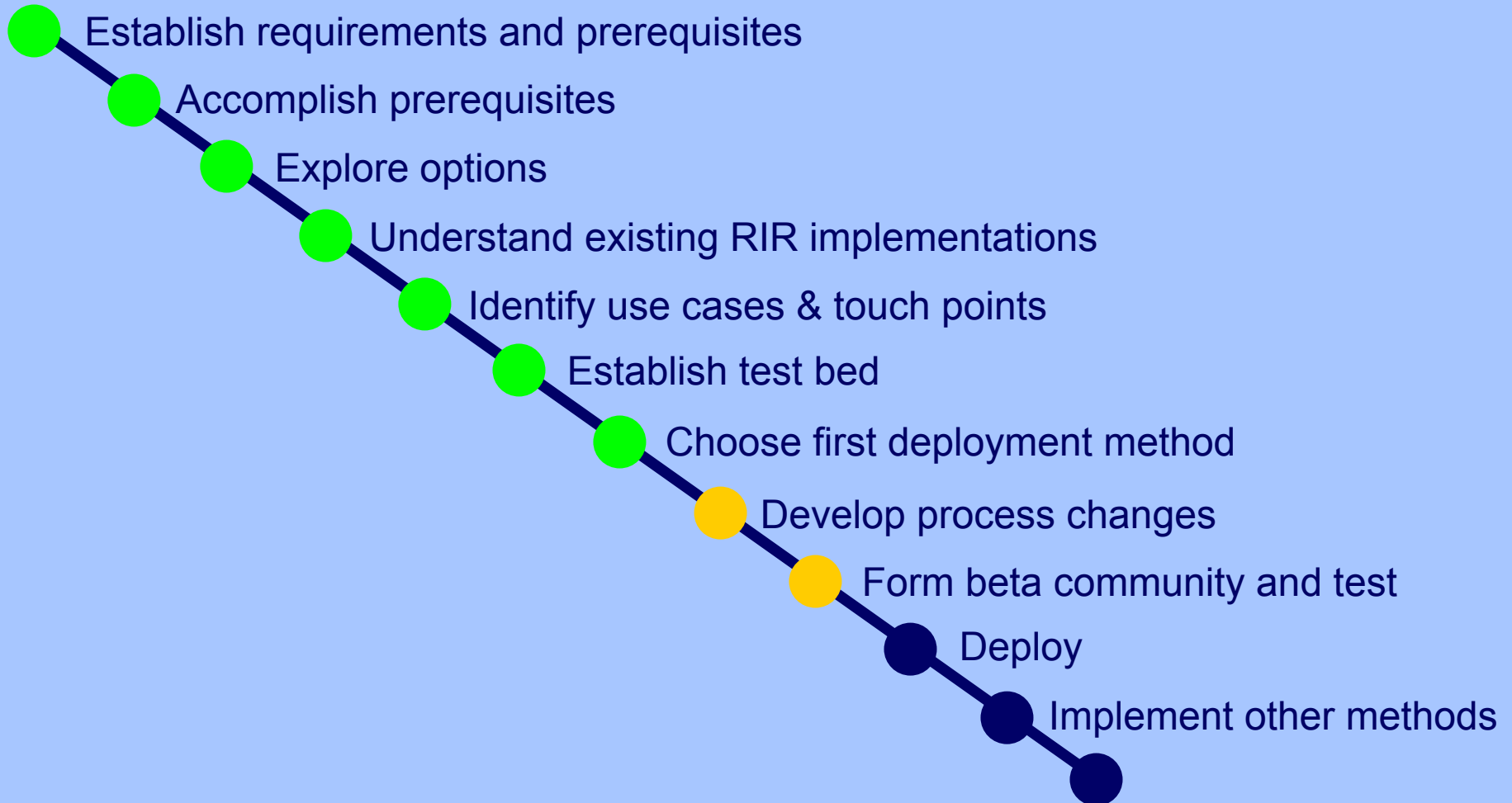
Interested? beta@arin.net

Perform beta training & testing
Refine/respond to beta issues
Training (internal/external)

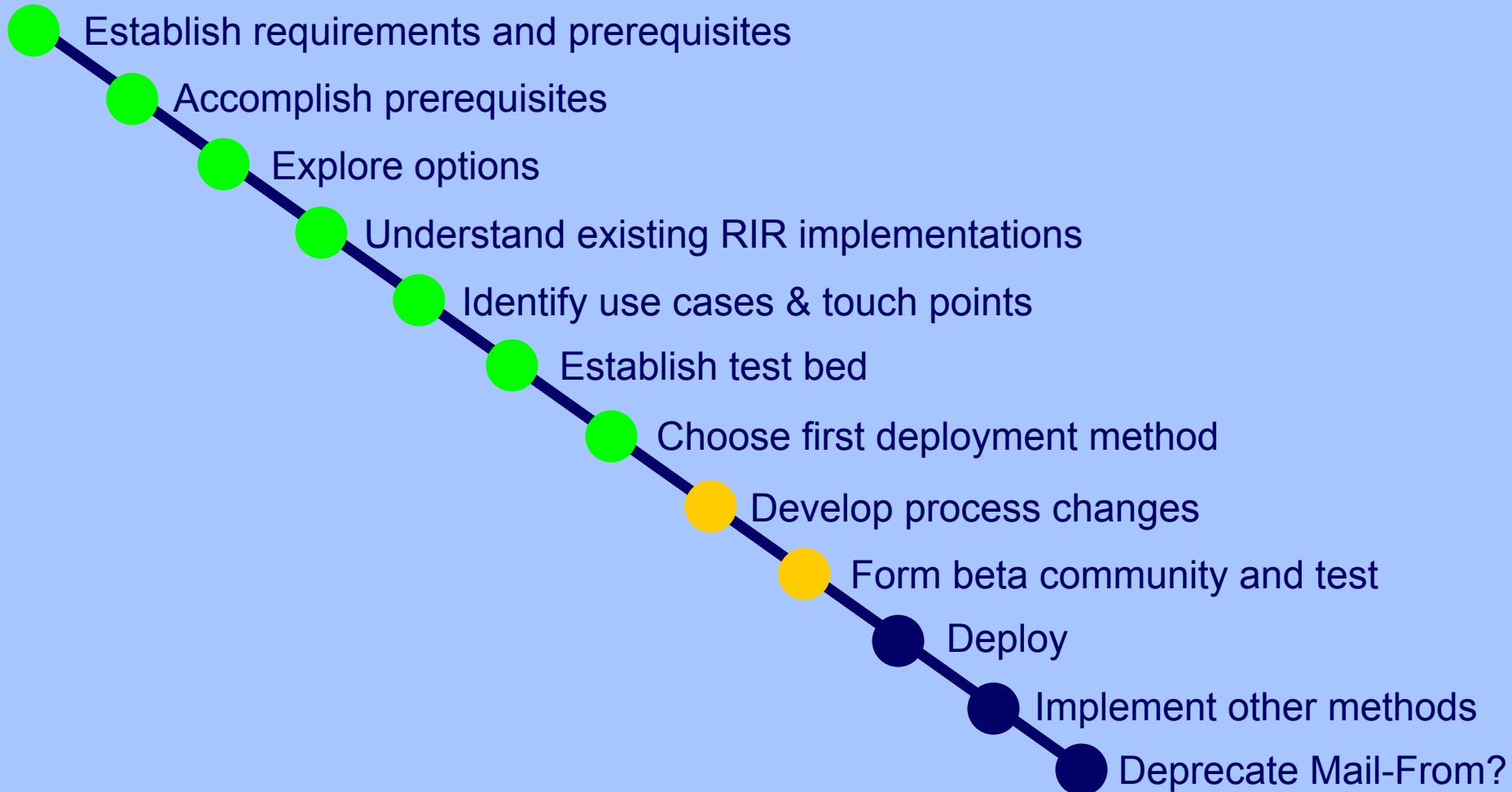
Timeline



Timeline



Timeline



Thank You!