What Happens When I Don't Have My Token?

Failover Strategies for Multi-Factor Authentication

David Walker
dhwprof@gmail.com

MFA Cohortium Meeting
7/24/2013

The Problem

- A user is required to use a hardware token to authenticate for a service but does not have the token available.
- Depending on the service, this could represent a serious business continuity issue.
- What options, other than denying service, are available?

Why Do You Have Multi-Factor Authentication?

- Opt-in for users to mitigate risks to them. Relying Parties don't require MFA.
    - Strategies need to meet user expectations.
- Required by Relying Parties, as part of a (formal or informal) assurance profile. Users don't have a choice, if they use those applications.
    - Strategies need to meet Relying Party expectations.
- And, of course, there are hybrids.

Potential Failover Strategies for Opt-In MFA

- Pre-registered proxies, friends or colleagues who are authorized to remove an MFA opt-in.
- A list of passwords that can each be used once for a single authentication event, overriding the MFA opt-in.
- Should the Relying Party be informed somehow when this happens?

Potential Failover Strategies for MFA Required by a Relying Party

- Relying Party provides access with restricted privileges.
  - May be no better than providing no access, depending on the situation.
- Relying Party provides "emergency" access for a limited period of time.
  - *E.g.*, doctors assisting at an airplane crash.
- Alternatives built into the assurance profile
  - Full or partial re-registration as part of authentication event.
  - Trusted third-parties that validate identity during an authentication event.

Other Ideas?

- Other use cases?
- Other issues?
- Other potential strategies?
- Is the Deployment Strategies subgroup willing to draft a white paper?